



The eG Getting Started Guide

eG Enterprise v5.6

Restricted Rights Legend

The information contained in this document is confidential and subject to change without notice. No part of this document may be reproduced or disclosed to others without the prior permission of eG Innovations Inc. eG Innovations, Inc. makes no warranty of any kind with regard to the software and documentation, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose.

Trademarks

Microsoft Windows, Windows NT, Windows 2000, Windows 2003 and Windows 2008 are either registered trademarks or trademarks of Microsoft Corporation in United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Copyright

© 2012 eG Innovations, Inc. All rights reserved.

The copyright in this document belongs to eG Innovations, Inc. Complying with all applicable copyright laws is the responsibility of the user.

Table of Contents

PURPOSE	1
ADMINISTERING EG ENTERPRISE	2
2.1 TARGET ENVIRONMENT.....	3
2.2 INSTALLING AND CONFIGURING THE EG MANAGER	4
2.3 ADMINISTERING EG ENTERPRISE	5
2.3.1 <i>Configuring Components</i>	9
2.3.2 <i>Configuring Services</i>	21
2.3.3 <i>Adding New Users</i>	27
2.3.4 <i>Configuring Tests</i>	34
INFRASTRUCTURE MONITORING USING EG ENTERPRISE	43
3.1 INSTALLING AND CONFIGURING EG AGENTS	43
3.2 INFRASTRUCTURE MONITORING USING EG ENTERPRISE	44
CONCLUSIONS	60

Table of Figures

Figure 2.1: Stages involved in deploying eG Enterprise	2
Figure 2.2: A target environment for deploying and testing eG Enterprise.....	3
Figure 2.3: The login window of eG Enterprise	6
Figure 2.4: The admin home page	6
Figure 2.5: Inputs to be specified for the discovery process.....	10
Figure 2.6: Changing the port preferences for discovery.....	10
Figure 2.7: Changing the general preferences for discovery	11
Figure 2.8: Managing / Unmanaging servers	13
Figure 2.9: Managing / Unmanaging MS SQL database servers	13
Figure 2.10: Selecting the type of component to add.....	14
Figure 2.11: Adding a Tomcat server	14
Figure 2.12: Adding a network node.....	16
Figure 2.13: List of remote agents	16
Figure 2.14: Configuring a remote agent.....	16
Figure 2.15: Clicking on the 'MODIFY' button to change the S SQL server's configuration	17
Figure 2.16: Enabling Agentless Monitoring of the MS SQL server	18
Figure 2.18: Specifying the details of a new segment	19
Figure 2.19: Configuring the segment topology	20
Figure 2.20: Adding a new service.....	21
Figure 2.21: Configuring a web site.....	22
Figure 2.22: Site topology of demo_service.....	24
Figure 2.23: Configuring transactions.....	25
Figure 2.24: Configuring the <i>upload</i> transaction for the site <i>demo_service</i>	25
Figure 2.25: Configuring the <i>Images</i> transaction for the site <i>demo_service</i>	26
Figure 2.26: All configured transactions are being displayed.....	26
Figure 2.27: Adding a new user	29
Figure 2.28: Configuring the services/segments/zones/components to be assigned to user <i>john</i>	34
Figure 2.29: Tests that need to be configured	35
Figure 2.30: Configuring the SQL Network test	36
Figure 2.31: The VIEW window	37
Figure 2.32: Configuring the SQL Database Space Test	38
Figure 2.33: Configuring the Java Server Web Access test	38
Figure 2.34: Configuring the JVM Memory Usage test	39
Figure 2.35: Configuring the Processes test.....	41
Figure 2.36: Configuring the Network Interfaces test	42
Figure 3.1: The Monitor Home page	44
Figure 3.2: Viewing the list of services in a particular state	45
Figure 3.3: Viewing the user-service mappings	46
Figure 3.4: Viewing the segments in a Normal state.....	46
Figure 3.5: Viewing the list of components in a particular state	47
Figure 3.6: The Event Analysis tab page	48
Figure 3.7: Viewing the list of components of a particular type.....	49
Figure 3.8: The Monitor menu	49
Figure 3.9: The list of segments that have been configured for our target environment	49
Figure 3.10: Viewing the user-segment mappings	50
Figure 3.11: The Service Dashboard that appears when the demo_service(Site) is clicked	50
Figure 3.12: The Transaction tab page of the Service Dashboard.....	51
Figure 3.13: The topology of the site <i>demo_service</i>	51
Figure 3.14: Measures pertaining to the Processes Test	52
Figure 3.15: Measures reported by the HttpTest for an IIS web server.....	53
Figure 3.16: The eG alarm window.....	53
Figure 3.17: Contents of the Alarm window	54
Figure 3.18: Viewing the details of the first alarm	55
Figure 3.19: Measures pertaining to the WindowsServices test	56
Figure 3.20: Measures pertaining to the Http test.....	56
Figure 3.21: Alarms pertaining to user <i>john</i>	57
Figure 3.22: Services associated with user <i>john</i>	57

Figure 3.23: A message indicating that no segments have been assigned to user <i>john</i>	58
Figure 3.24: Alarm window displaying no alarms	58
Figure 3.25: Measures reported by the WebServerTest	59

Purpose

The purpose of this document is to quickly lead the reader through a series of steps that will enable him/her to deploy, test, and understand the working of eG Enterprise.

For a detailed understanding of all the features of eG Enterprise, the reader is referred to the following documents:

-  *The eG User Manual*
-  *The eG Measurements Manual*
-  *The eG Installation Guide*
-  *A Virtual Private Monitoring and Optimization Solution for Multi-Domain IT infrastructures*

Administering eG Enterprise

Deploying eG Enterprise in a target IT Infrastructure is a very simple task. The different steps involved in deploying eG Enterprise in a Windows environment are:

1. **Installation and Configuration** of the eG manager and the agents: This stage mainly involves deployment of the software on the appropriate servers in the infrastructure and setting up the environment for the proper operation of the eG manager and agent.
2. **Administration** of eG Enterprise: At this stage, the user interacts with the eG manager through the eG user interface to determine where agents must be deployed, what tests these agents must run, how often the tests should run, etc. In addition, new users are added to or deleted from eG Enterprise at this stage.
3. **Monitoring** using eG Enterprise: At this stage, using the user interface, users can monitor various aspects of their IT infrastructure.

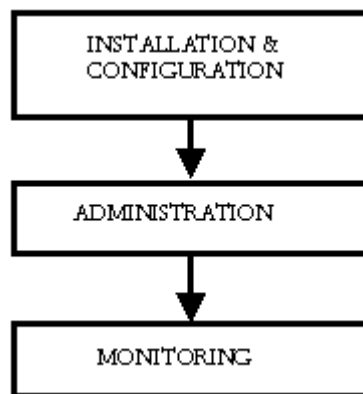


Figure 2.1: Stages involved in deploying eG Enterprise

Figure 2.1 depicts the various stages involved in deploying eG Enterprise in a target environment. Using illustrative examples, the following sections explain these stages in detail.

2.1 Target Environment

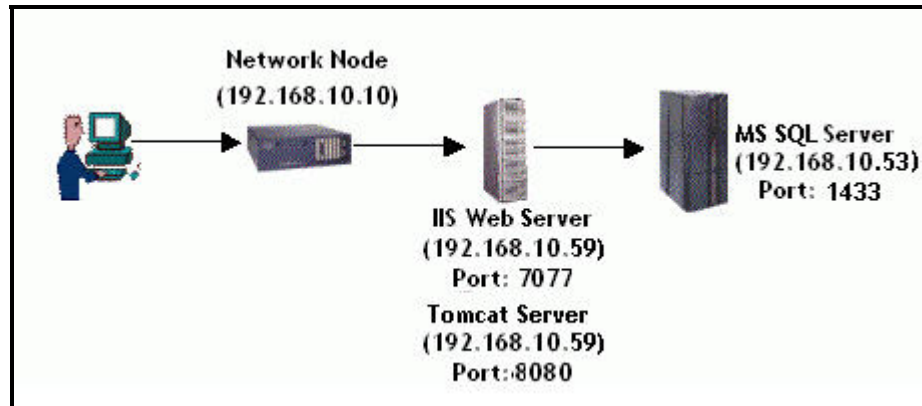


Figure 2.2: A target environment for deploying and testing eG Enterprise

To illustrate the deployment and testing of eG Enterprise, in this document, we use the target environment shown in Figure 2.2. The target environment comprises of a network node (192.168.10.10), a system that hosts an IIS web server and a Tomcat server (192.168.10.59), and a third system (192.168.10.53) that hosts an MS SQL database server. The eG manager that monitors this environment has been installed on the web server, 192.168.10.63:7077.

The table below discusses where agents have been deployed in the target environment, and what applications they monitor:

Agent Host	Component(s) Managed	Agent Type
192.168.10.59	IIS web server: 192.168.10.59:7077	Internal
	Tomcat server: 192.168.10.59:8080	Internal
192.168.10.63	MS SQL server: 192.168.10.53:1433	Remote
192.168.10.63	IIS web server: 192.168.10.59:7077	External
	Tomcat server: 192.168.10.59:8080	External
	MS SQL server: 192.168.10.53:1433	External
	Network node: 192.168.10.10	External

The IIS web server (192.168.10.59:7077), Tomcat server (192.168.10.59:8080), and the MS SQL server (192.168.10.53:1433) have been externally managed by the agent deployed on the 192.168.10.63. Also, the agent on 192.168.10.63 doubles as a remote agent, and internally monitors the MS SQL server at 192.168.10.53:1433.

The following sections describe the steps involved in configuring eG Enterprise for this target environment. Illustrative examples are also provided to explain how the reader can test the functionality of eG Enterprise.

2.2 Installing and Configuring the eG Manager

1. **Verifying prerequisites:** Chapter 3 of the *eG Installation Guide* lists the prerequisites for installing the eG manager. Verify these prerequisites before getting started. Briefly, the eG software for Windows environments requires the following:
 - Windows 2003 server (OR) Windows 2008 server (OR) Windows XP workstation (OR) Windows 7
 - Oracle database server (version 10G or higher) / Microsoft SQL Server (version 2005 / 2008 / 2012) for the eG database
 - JDK 1.5 (or its variants) / JDK 1.6.0_10 and above
 - A minimum of 1 GB of disk space free
 - A minimum of 2 GB RAM would be required for installing the eG manager on a 32-bit host; for a 64-bit host on the other hand, a minimum of 4 GB RAM would be required

For Unix environments, the eG software requires the following:

- Solaris 10 (or higher) or Red Hat Linux 6.0
- JDK 1.5 (or its variants) / JDK 1.6.0_10 and above
- Oracle database server (version 10G or higher) / Microsoft SQL Server (version 2005 / 2008 / 2012) for the eG database
- A minimum of 1 GB of disk space free
- A minimum of 2 GB RAM would be required for installing the eG manager on a 32-bit host; for a 64-bit host on the other hand, a minimum of 4 GB RAM would be required

In our target environment, the eG manager has been installed on the Windows system, 192.168.10.63, and listens on the port 7077.

2. **Installing and Configuring the eG manager:** The eG manager is the central unit that is responsible for coordinating the functioning of the agents, analyzing the reports from the agents to determine whether any problems exist, and for handling user requests to eG Enterprise. eG Enterprise manager setup software is provided as a self-extracting executable program called **eGManager.exe** that can be installed and configured on the Windows operating systems. On Solaris environments it is available as a standard Solaris package (named **eGmanager**) that can be installed using the **pkgadd** utility. For installation on Linux systems, the eG manager is provided as a tar file (named **eGmanager.tar**). The installation process is driven by a shell script named **iManager**. Administrator privileges are required to install the eG manager. Before proceeding with the installation process, please go to Control Panel-> Display->Settings in Windows environments and set the number of colors to **65536** at least. This is the optimal **Display** setting in the computer to view the eG User Interface well. For the detailed installation procedure, please refer to Chapter 2 and Chapter 3 of the *eG Installation Guide*.
3. **Starting the eG manager:** The eG manager has to be started next. Before starting the manager, make sure that you have a valid file named **license** in the **<EG_HOME_DIR>\bin** (the **/opt/egurkha/bin** directory in Unix environments) directory. To start the manager, click the **Start** button on the task bar. From thereon, select Programs > eG Monitoring Suite > eG Manager > Start Manager. In Unix environments, execute the command **/opt/egurkha/bin/start_manager**.

Note:

The steps for administering and monitoring eG Enterprise discussed below **are specific to a Windows environment**. eG Enterprise on a Unix environment can be administered and monitored in a similar manner.

2.3 Administering eG Enterprise

Following the installation and configuration of the eG manager, the next step is to administer eG Enterprise.

1. To start administering eG Enterprise, first access eG Enterprise using a web browser. Connect to the URL `http://192.168.10.63:7077/`, (If the manager were SSL-enabled, then you would have to use the URL: `https://192.168.10.63:7077/`).

Note:

While specifying the URL, please take care of the following aspects:

- a. If the host name is provided when installing the manager, use this name (and not the IP address) for accessing the user interface via the web browser.
- b. If the host name is provided, make sure that forward and reverse lookups for this name are enabled via the DNS service in the target environment.

2. The eG login window appears (see Figure 2.3). eG Enterprise comes with a predefined administrator account with login name *admin* and password *admin*. Specify the same in the respective text boxes in Figure 2.3 and click the **AUTHENTICATE** button to proceed.

Administering eG Enterprise



Figure 2.3: The login window of eG Enterprise

3. Upon successful login, the **ADMIN HOME** page will appear.

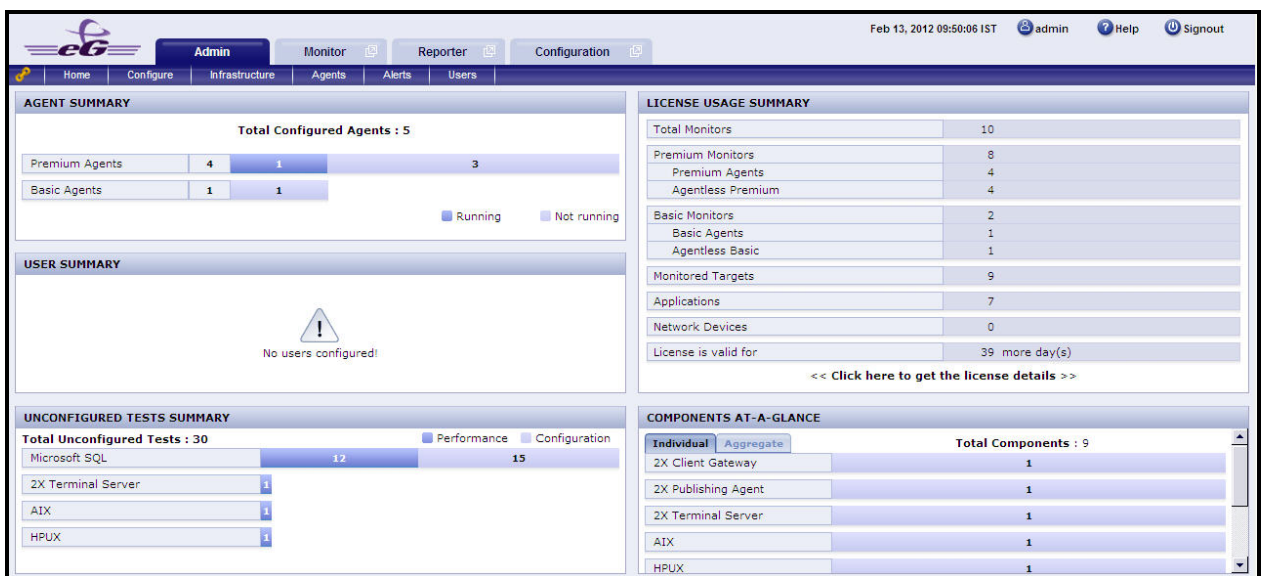


Figure 2.4: The admin home page

Administering eG Enterprise

This page enables the administrator to understand, at a glance, the status of the eG monitoring system. The page reveals the following information:

- The first section of the page provides the **AGENT SUMMARY** (see Figure 2.4). This section displays the total number of agents that have been configured for the environment. The number of agents of each type (Basic and Premium) that have been configured, and the number of agents that are currently running/not running are also indicated. Clicking on a bar corresponding to Premium or Basic agents will lead you to the agent **STATUS** page that lists all the agents of the corresponding type, and their current status.
- Below the **AGENT SUMMARY** is the **USER SUMMARY** (see Figure 2.4). This bar graph indicates the number of **Expired** user accounts, user accounts which are **Nearing Expiry** (i.e. the accounts that will expire within 7 days), and **Others**. The **Others** bar includes the number of users who will never expire (i.e. users for whom the **No Expiry** option has been set), and the number of users who are not expected to expire within the next 7 days. Clicking on any of the bars in this section takes you to a page that reveals the list of users who belong to the category “clicked on”, and displays the components, segments and services (if any) that have been associated with each of the users. Users are yet to be created for our target environment. Therefore, this again will not provide a summary.
- For each component (i.e. network device or application) being monitored, eG includes a specialized model that dictates what tests must be run by the eG agent to monitor the component. Many of eG’s tests are pre-configured i.e., do not require manual configuration. A few tests require explicit configuration. The third section in the **Admin Home** page provides the **UNCONFIGURED COMPONENT SUMMARY** (see Figure 2.4). Besides providing the total number of unconfigured tests, this section graphically depicts the number and type of components for which tests remain to be configured. For more information on the unconfigured tests, click on the bar that corresponds to a component type. This will take you to the **LIST OF UNCONFIGURED TESTS** that provides the complete list of tests requiring manual configuration for the chosen component type. No components have been managed yet for our target environment. Therefore, this summary will also be empty.
- Finally, you have the **LICENSE USAGE SUMMARY** (see Figure 2.4). The eG license governs a wide variety of factors such as the number and type of agents that the installation can support, the number of applications that can be monitored, etc. The information provided by the **LICENSE USAGE SUMMARY** helps the administrator assess whether the eG licenses are being effectively utilized. Clicking on the **LICENSE DETAILS** button here will take you to the **LICENSE INFORMATION** page that provides the license details as well as its usage details.
- Finally, a **COMPONENTS AT-A-GLANCE** section is available, which indicates the component-types that are currently monitored by eG Enterprise, and the number of managed components per type. Clicking on the bar corresponding to a component-type leads you to the **ADD/MODIFY** page where more components of that type can be added for monitoring.

At the top of the Admin Home page is a menu bar (see Figure 2.4) that offers the following options:

- **Configure:** This menu allows an administrator to perform the following functions:
 - Use the Integration Console to extend the capabilities of the eG Enterprise suite to monitor new/in-house/legacy applications; **this is a license-controlled capability, and hence, will be available only if your eG license enables it.**
 - Choose the measures for which Operation reports need to be generated in the eG Reporter; **the eG Reporter component will be available to you only if your eG license enables it.**
 - Configure the database cleanup schedule
 - Define the frequency of detailed diagnosis measures; **this is a license-controlled capability, and hence, will be available only if your eG license enables it.**

Administering eG Enterprise

- Configure a supermanager, which will serve as a single point of control, if multiple managers are configured in your environment; **this is a license-controlled capability, and hence, will be available only if your eG license enables it.**
- Define the manager and logging settings
- Define settings for the eG monitoring console
- Effect cosmetic changes to the eG admin and monitor interfaces by including custom logos and defining custom alert messages
- **Infrastructure:** This menu enables the administrator to discover, manage, and add/modify components to the eG Enterprise system, configure zones, services, segments, component groups, and component topologies.
- **Agents:** The options provided by this menu allows you to:
 - Configure tests to be executed on target components, so as to extract performance data from them
 - Enable/disable test descriptors
 - View the status of agents
 - Define the manager-agent communication settings, and configure remote control commands; **remote control is a license-controlled capability and will be available only if your eG license enables it.**
 - Configure external agents and assign hosts to them
 - Configure remote agents and assign hosts to them; **this option will be available only if your eG license enables 'Agentless Monitoring'.**
 - Assign agents to primary and secondary managers in Active-Active redundant manager cluster; **this option will be available only if your eG license enables the 'Redundant Manager' capability.**
 - Define auto-upgrade settings
- **Alerts:** This menu enables the administrator to do the following:
 - Configure thresholds, which govern state changes
 - Define the alarm policies, based on which the eG Enterprise system will generate alarms
 - Add/modify/delete maintenance policies, which when defined, can suppress the alarms pertaining to specific hosts/components for configured time periods
 - Configure the mail server for generating alarms
 - Configure SNMP traps, using which eG Enterprise can integrate with third-party network management systems (eg., HP OpenView) that might pre-exist in a target environment
- **Users:** This menu enables the administrator to do the following:
 - Create and manage the users to the eG system
 - Configure user roles for the created users
 - Configure domain settings for the users
 - View the users who are currently logged in to the eG system, the details of the user, the services assigned to the particular user and the expiry of the user

Administering eG Enterprise

- **Audits:** eG Enterprise can be optionally configured to log every user action performed on the eG user interface. Using the **Audits** menu, a variety of reports can then be generated based on the details logged, so as to enable the administrator to audit the following:
 - User logins to the eG Enterprise system
 - Failed login attempts to the eG Enterprise system
 - Configuration changes effected by users to the eG administrative interface
 - User activities with respect to the eG monitoring console
 - User accesses to the eG Reporter module

By default, the 'audit logging' capability of the eG manager is disabled. Therefore, the Audits menu will not be available by default.

Clicking on the **Signout** option on the right, top corner of this page will allow the administrator to log out of the administrative interface. Click on the **Profile** button to modify the profile of the current login user. If you click on the **Help** button here, a context-sensitive help page providing useful information pertaining to the page that is currently open, will appear.

If your user profile has monitoring rights, then a **Monitor** tab will appear, clicking on which will enable you to login to the eG monitoring console, without having to log out of the admin interface. Similarly, if you have rights to generate reports, then a **Reporter** tab will appear, clicking on which will allow you to instantly switch to the eG Reporter interface (if your eG license enables it). By default, clicking on either of these tabs will open the monitor and reporter interfaces in the currently open window itself. If you want these consoles to open in a separate window instead, click on the  symbol next to the tab page name **Monitor** or **Reporter** as the case may be.

2.3.1 Configuring Components

In order to enable infrastructure monitoring, the components in the target environment and the inter-dependencies among them have to be configured. This section describes the steps involved in configuring the components to be monitored.

1. By clicking on the **INFRASTRUCTURE** menu option, followed by the option **Components** option, and then the **Discover** option, the user can reach a point where he/she can start configuring the components to be monitored in the target environment.
2. The components in the environment have to first be discovered. The **START DISCOVERY** page (see Figure 2.5) that appears when the above-mentioned menu sequence is followed, will enable administrators to automatically discover the components in the target environment. Click the **Ports** sub-node of the **Settings** node in the tree-structure to alter the preferences associated with discovery of the different components. Figure 2.6 depicts the **START DISCOVERY >> CHANGE PREFERENCE** screen.

DISCOVERY

- Discovery
 - Start Discovery
 - Stop Discovery
 - Manage Components
 - Settings
 - General
 - Ports
 - SNMP Communities
 - vCenters
 - View
 - Add/Discover
 - Modify/Discover
 - Delete
 - Configure
 - HMCs
 - View
 - Add/Discover
 - Modify/Discover
 - Delete
 - RHEV Managers
 - View
 - Add/Discover
 - Modify/Discover
 - Delete
 - Public Clouds
 - View
 - Add/Discover
 - Modify/Discover
 - Delete

START DISCOVERY

This page enables the administrator to start discovering the components in the monitored environment.

IP range : 192.168.10.1-192.168.10.30
eg : (172.15.16.1-172.15.16.30, 192.68.10.1-192.68.10.30)

Components : 2X Client Gateway, 2X Publishing Agent, 2X Terminal Server, 3Com Core Builder, AGate, AIX, Alcatel Switch, Apache Web, APC UPS, AS400

Start Discovery

Figure 2.5: Inputs to be specified for the discovery process

DISCOVERY

- Discovery
 - Start Discovery
 - Stop Discovery
 - Manage Components
 - Settings
 - General
 - Ports
 - SNMP Communities
 - vCenters
 - View
 - Add/Discover
 - Modify/Discover
 - Delete
 - Configure
 - HMCs
 - View
 - Add/Discover
 - Modify/Discover
 - Delete
 - RHEV Managers
 - View
 - Add/Discover
 - Modify/Discover
 - Delete
 - Public Clouds
 - View
 - Add/Discover
 - Modify/Discover
 - Delete
 - AWS EC2 Cloud
 - View
 - Add/Discover
 - Modify/Discover
 - Delete

START DISCOVERY >> CHANGE PREFERENCE

This page enables the administrator to configure the ports to be used for application discovery.

PORT SETTINGS	
2X Publishing Agent	: 20002
2X Terminal Server	: 30004
AGate	: 3900
AIX	: 23
BlackBerry 4x	: 3101
Cache Database	: 1972
CheckPoint	: 18184
Citrix License	: 7279
Citrix MF	: 1494
Citrix Provisioning Server	: 54321
Citrix XenApp	: 1494,2598
DB2 DPF	: 50000
DB2 UDB	: 50000
DNS	: 53
Domain Controller	: 88
Domino Mail	: 25

Update

Figure 2.6: Changing the port preferences for discovery

- In the target environment of Figure 2.2, the IIS web server is listening to requests on port 7077. In order to discover this web server automatically using the eG manager, add the port number 7077 in the **Web server** text box in Figure 2.6. Click the **Update** button to register the changes.

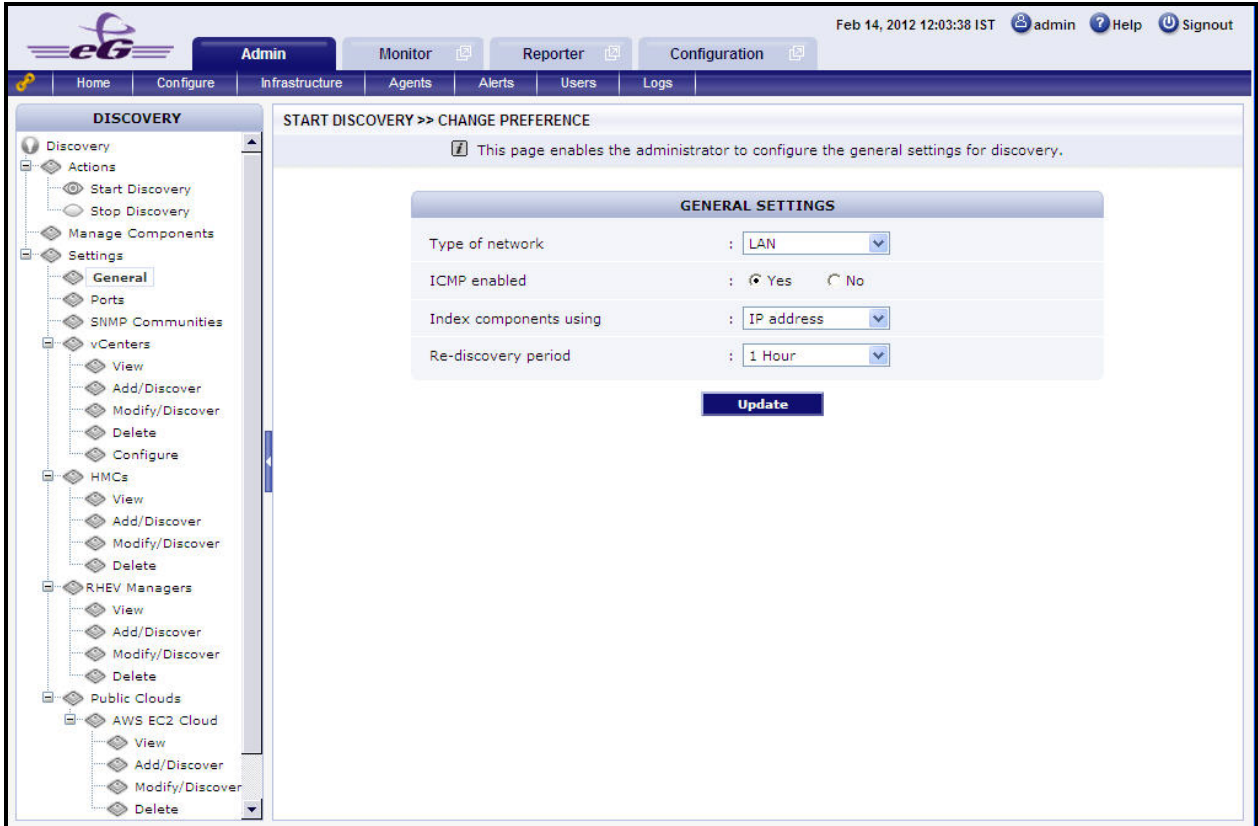


Figure 2.7: Changing the general preferences for discovery

4. Click on the **GENERAL** sub-node from the **SETTINGS** node in the tree structure of the **START DISCOVERY** page to alter the general preferences for discovering the components in the target environment. From the **Type of Network** list box in Figure 2.7, the administrator can choose the type of network being discovered. The default choice is a Local Area Network (LAN), wherein network delays are of the order of a few tens of milliseconds. To support networks that span multiple geographic locations, an administrator can change the network type to a Wide Area Network (WAN) in which case, the network delays are of the order of seconds. By default, the eG manager attempts to use the Internet Control Message Protocol (ICMP) to figure out which hosts are available in the target environment. Once the hosts that are available are detected, the manager uses a simple port scanning technique to discover the components running on these hosts. For security reasons, some environments may not allow ICMP traffic through their networks. An administrator can inform the eG manager of such a restriction by using the **ICMP enabled** option. If this value is set to "No", the eG manager directly uses the port scanning technique for each of the hosts in the specified IP address ranges.

The discovered components can be represented either using IP addresses or using domain names. In the latter case, when it discovers a component, the eG manager queries the Domain Name System to resolve an IP address to a domain name. The **Index components using** option directs eG Enterprise to either use the IP address itself to identify a server (the choice of "IP Address") or to use the domain name (the choice of "Host Name"). Use the "Host Name" option only if the target environment is configured properly to use the Domain Name System (i.e., both name to IP address and IP address to name mappings are specified in the DNS). The administrator can choose one of the two options from the **Index components using** list box. The **Re-discovery period** in Figure 2.7 determines the frequency with which the discovery process executes.

This frequency governs how quickly the eG manager is able to discover components that may have been newly added to the target environment.

Note:

The selection from the **Index components using** drop-down of Figure 2.7, and the **Re-discovery** period indicated therein do not just apply to general component discovery, but also to the following types of discovery that can be performed using the **DISCOVERY** page:

- the discovery of vSphere/ESX servers via vCenter;
- the discovery of IBM pSeries servers via HMC server;
- the discovery of Public clouds;
- the discovery of RHEV servers via the RHEV manager

5. Now, in the **START DISCOVERY** page (see Figure 2.5), specify the range of IP addresses of the target environment in the **IP range** text box. As you can see in Figure 2.5, the components that eG Enterprise can discover is available in the **Components** list box. Finally, click the **Start Discovery** button in Figure 2.5 to start the discovery process.

Figure 2.5 provides an example of the inputs that need to be specified in case the target environment comprises of more than one IP address range. For more information on the other options available for discovery, use eG Enterprise's context-sensitive help capability. Clicking on the "? **Help**" in top panel of Figure 2.5 will provide the user with details on each of the input fields of Figure 2.5.

6. eG agents run the tests only on the components that are managed. Choose the **Components -> Manage/Unmanage** option from the **Infrastructure** menu to manage the components that have been discovered by eG Enterprise's discovery process. The screen shown by Figure 2.8 appears. In this screen, first choose the component type (**IIS Web**) from the list box available in this page. For the first time, all the components discovered will appear in the **UNMANAGED COMPONENTS** list box. Select the server to be managed and then click the << **Manage** button. This server will now move over to the **MANAGED COMPONENTS** box. Clicking on the **Update** button will register the changes made. Figure 2.8 shows that the web server under consideration, 192.168.10.59:7077 has been managed.

Administering eG Enterprise

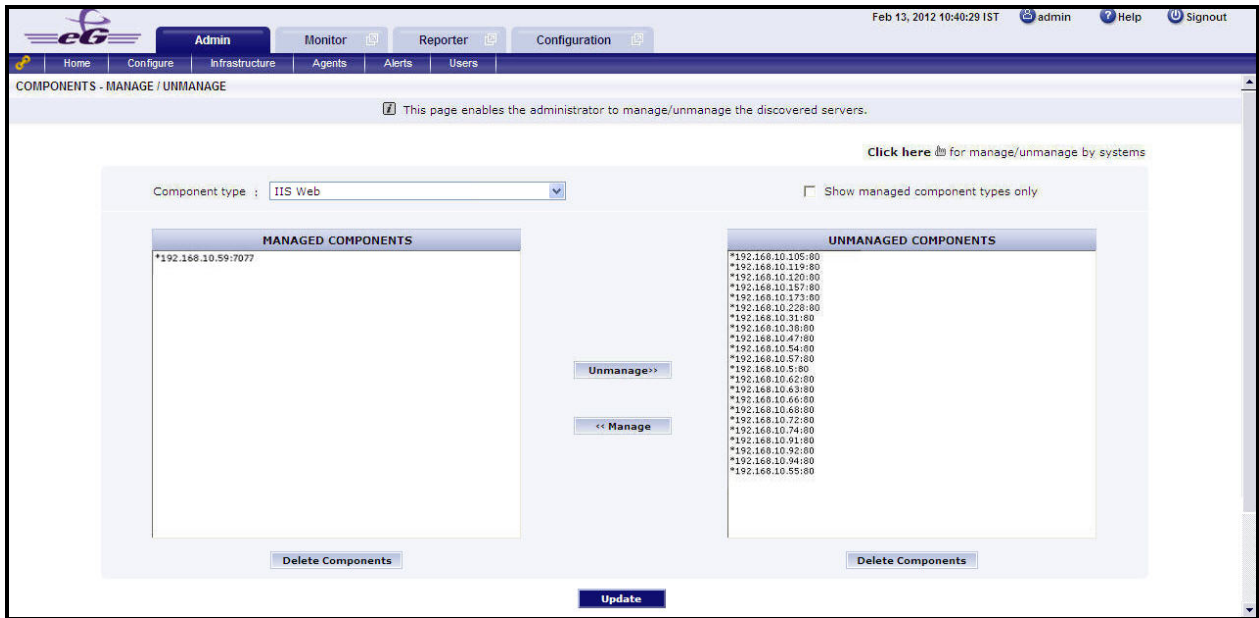


Figure 2.8: Managing / Unmanaging servers

- To manage the MS SQL database server 192.168.10.53:1433, choose **Microsoft SQL** from the **Component type** list box in Figure 2.9.

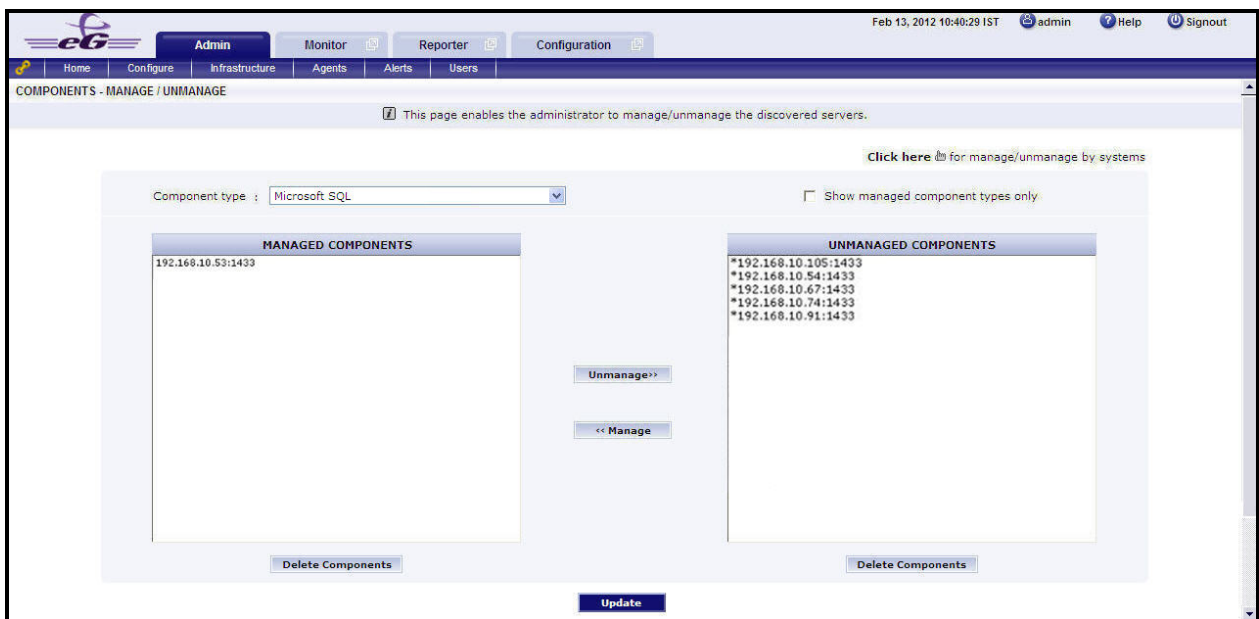


Figure 2.9: Managing / Unmanaging MS SQL database servers

- Components that are not discovered by the discovery process can be manually added to the eG Enterprise system using the **Components** -> **Add/Modify** option in the **Infrastructure** menu. Such components will be automatically managed by the eG Enterprise system. Let us now add the Tomcat server, 192.168.10.59:8080, in our target environment, using this option. Once the **Add/Modify** option is selected, Figure 2.10 appears. Select **Tomcat** from the **Component type** list box and click the **Add New Component** (see Figure 2.10) button.

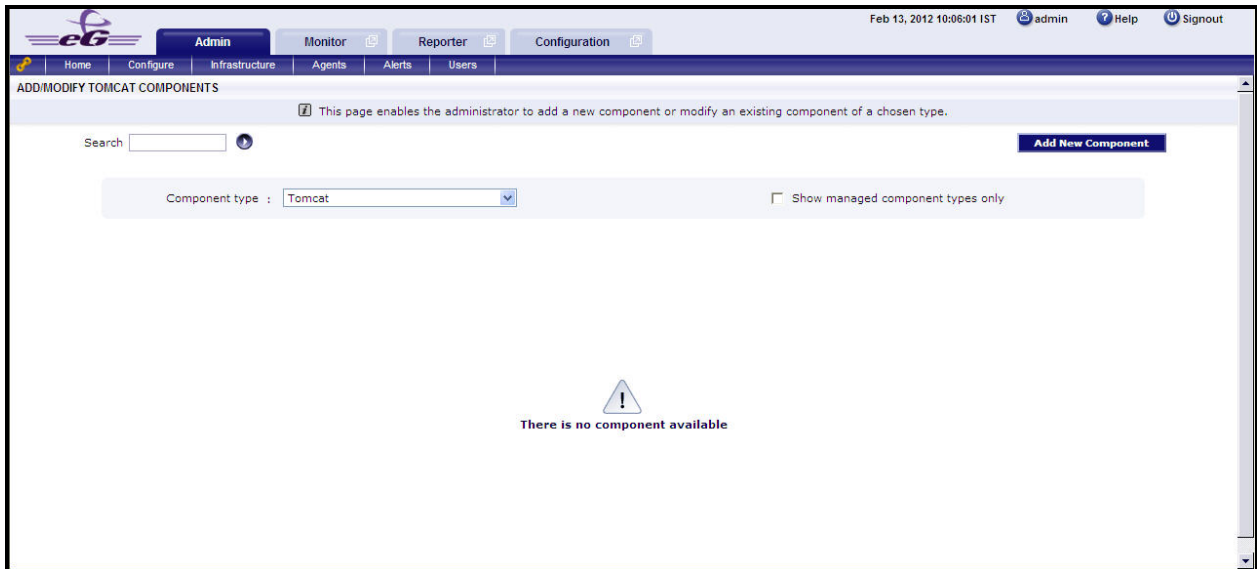


Figure 2.10: Selecting the type of component to add

9. In the **NEW COMPONENT DETAILS** page that appears next, provide the IP of the Tomcat server in the **Host IP** text box. Then, specify a valid **Host name** for the Tomcat server. Here, an administrator has the option of specifying a **Nick name** instead of the host name. A nick name is a logical name that is associated with the host being monitored. This nick name should be the same as that provided while installing the agent on the host. Figure 2.11 will also display the default **Port number** of the Tomcat server, which is 8080.

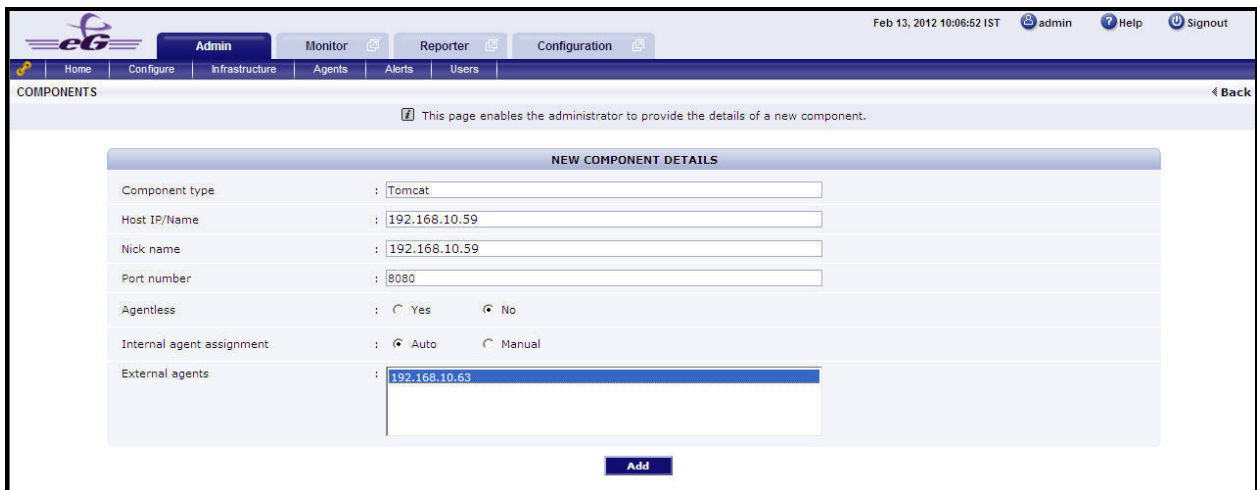


Figure 2.11: Adding a Tomcat server

When adding any new application/system for monitoring, administrators have a choice of whether to use agent-based or agentless monitoring for the application or system under consideration. For instance, an administrator can choose to monitor the most critical servers in an agent-based manner, and to monitor the less critical servers in the staging/development environment in an agentless manner. In the agentless monitoring approach, environments are monitored from remote locations - i.e., external to the system or application that is to be monitored. The main advantage of this remote monitoring approach is that it does not require an agent to be installed

on every system that is to be monitored. To enable/disable agentless monitoring for a component, select the **Yes** or **No** options against **Agentless** (see Figure 2.10), as the case may be. This option appears only if at least one remote agent has been configured for the target environment. **Remote Agents** are agents using which eG implements agentless monitoring. If no remote agents have been configured, then agent-based monitoring is used by default. For more information on remote agents and agentless monitoring, refer to the *eG User Manual*. Since the target Tomcat server in our example is to be monitored using the traditional agent-based approach, select **No** against **Agentless**.

By default, if a host has multiple IP addresses, the eG Enterprise system requires one agent license for each IP address that is managed internally. Likewise, if multiple nicknames are used for the same IP address, a separate internal agent license is used for each unique nickname that has been specified. In many large environments, a single server has many IP addresses, each with different nicknames. The agent per system capability is intended to optimize the internal agent license usage in such large infrastructures. If this capability is enabled by the eG license, the administrator has the option of overriding the default eG agent licensing policy. By doing so, the administrator can ensure that a single agent license is sufficient to manage all the IP addresses and applications executing on a host. The **Internal agent assignment** field in the **NEW COMPONENT DETAILS** page of the eG administrative interface allows you to override the default agent licensing policy. By default, the **Auto** option against the **Internal agent assignment** field will be selected. This indicates that by default, eG maps every configured IP/nick name with a separate internal agent. To manually define the IP-internal agent association, select the **Manual** option. For the **Tomcat server** in our example, let us go with the default selection, **Auto**.

Note:

The **Internal agent assignment** field will appear only if the following conditions are fulfilled:

- The eG license enables the **Agent per system** flag
- The **Agentless** flag in Figure 2.11 is set to **No**. In other words, users will not have the option of mapping an IP to an internal agent, if agentless monitoring is enabled.

Finally, associate one or more **External agents** with the component. In the target environment in our example, 192.168.10.63 is the agent that will externally monitor the **Tomcat server**, **192.168.10.59:7079**. Select the agent and click the **Add** button.

10. Similarly, add the network node 192.168.10.10 to the eG Enterprise system (see Figure 2.12).

Administering eG Enterprise

The screenshot shows the 'NEW COMPONENT DETAILS' form in the eG Enterprise administration interface. The form is titled 'NEW COMPONENT DETAILS' and contains the following fields:

- Component type: Network Node
- Host IP/Name: 192.168.10.10
- Nick name: 192.168.10.10
- External agents: 192.168.10.63

An 'Add' button is located at the bottom right of the form. The page header includes the eG logo, navigation tabs (Admin, Monitor, Reporter, Configuration), and user information (Feb 13, 2012 10:08:00 IST, admin, Help, Signout).

Figure 2.12: Adding a network node

11. Unlike the Tomcat and IIS web servers in our example which use the agent-based approach to monitoring, the MS SQL server, 192.168.10.53:1433, is to be monitored in an 'agentless manner' by the remote agent at 192.168.10.63. The first step towards enabling agentless monitoring for the MS SQL server is to configure the remote agent. To achieve this, first, follow the menu sequence: *Agents -> Remote Agents -> Configure*. Figure 2.13 will then appear listing the remote agents that have already been configured (if any).

The screenshot shows the 'REMOTE AGENT CONFIGURATION' page in the eG Enterprise administration interface. The page is titled 'REMOTE AGENT CONFIGURATION' and contains the following elements:

- A search bar with a dropdown arrow.
- An 'Add New Agent' button.
- A table listing remote agents:

IP Address	View	Delete
192.168.8.192	View	Delete
192.168.10.63	View	Delete

The page header includes the eG logo, navigation tabs (Admin, Monitor, Reporter, Configuration), and user information (Feb 13, 2012 11:21:59 IST, admin, Help, Signout).

Figure 2.13: List of remote agents

12. To configure a new remote agent, click on the **Add New Agent** button in Figure 2.13. Then, specify the IP address and nick name of the new remote agent in the space provided in Figure 2.14. Click the **Update** button to register the changes.

The screenshot shows the 'NEW REMOTE AGENT DETAILS' form in the eG Enterprise administration interface. The form is titled 'NEW REMOTE AGENT DETAILS' and contains the following fields:

- Agent IP Address: 192.168.10.63
- Agent Host/Nick Name: 192.168.10.63
- Add as External agent: ☐ Yes ☒ No

An 'Update' button is located at the bottom right of the form. The page header includes the eG logo, navigation tabs (Admin, Monitor, Reporter, Configuration), and user information (Feb 13, 2012 10:21:56 IST, admin, Help, Signout).

Figure 2.14: Configuring a remote agent

Administering eG Enterprise

13. Next, proceed to assign the remote agent to the MS SQL server. To do so, first, follow the *Infrastructure -> Components -> Add/Modify* menu sequence, select **Microsoft SQL** from the **Component type** list, and then click on the **Modify** button corresponding to the managed MS SQL server, 192.168.10.53:1433 (see Figure 2.15).

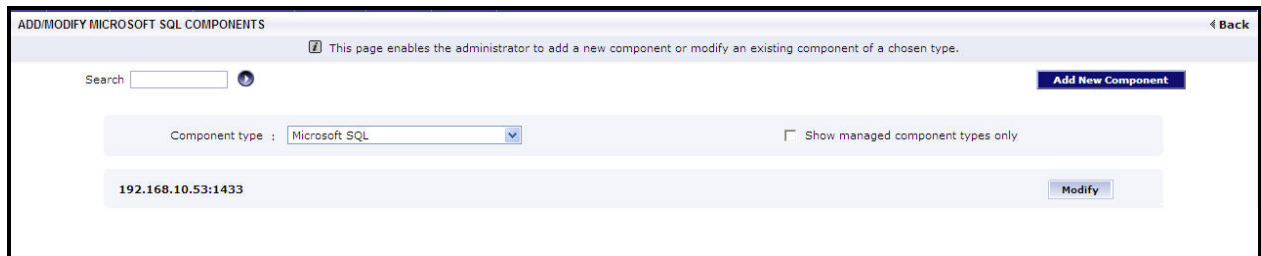


Figure 2.15: Clicking on the 'MODIFY' button to change the S SQL server's configuration

14. In the **MODIFY COMPONENT DETAILS** page that appears next (see Figure 2.16), select the **Yes** option against **Agentless** to allow agentless monitoring of the MS SQL server. Then, from the **OS** list box, select the Windows operating system on which the MS SQL server has been installed. Doing so will automatically display the **Perfmon** option in the **Mode** list box. A remote agent connects to the Windows host to be monitored using **NetBIOS** - a protocol that allows applications on different computers to communicate within a local area network. Then, it extracts measures from the host using the Windows Performance Monitoring utility, known as **Perfmon**. Since the **OS** selected in our example is a Windows operating system, the **Perfmon** option got selected by default. Next, select the 192.168.10.63 agent from the **Remote agent** list box - this should ensure that the MS SQL server in our example is monitored by the remote agent at 192.168.10.63. Since the remote agent 192.168.10.63 also functions as an external agent, select it once again from the **External agents** list. Finally, click the **Update** button to save the changes.

The screenshot shows the 'MODIFY COMPONENT DETAILS' form in the eG Enterprise administration interface. The form is titled 'MODIFY COMPONENT DETAILS' and contains the following fields:

- Component type: Microsoft SQL
- Host IP/Name: 192.168.10.53
- Nick name: 192.168.10.53
- Port number: 1433
- Is passive: ☐ Yes ☒ No
- Agentless: ☒ Yes ☐ No
- OS: Windows XP
- Mode: Perfmon
- Remote agent: 192.168.10.63
- External agents: 192.168.10.63

An 'Update' button is located at the bottom of the form.

Figure 2.16: Enabling Agentless Monitoring of the MS SQL server

Note:

Before attempting to monitor a Windows-based component in an agentless manner, refer to the *eG User Manual* for the **ports to be opened** and the **detailed list of pre-requisites** to be fulfilled for enabling the remote agent to collect measurements from Perfmon counters.

- Next, the interdependencies between the managed components have to be configured for eG Enterprise's correlation capabilities to function effectively. For this, you need to define the **TOPOLOGY**. Before actually proceeding with configuring the topology, one should understand that eG Enterprise supports two types of dependencies: the **Connects** dependency, which typically indicates flow of data (e.g., a physical connection between a web server and a network router), and the **Uses** dependency, which refers to a logical dependency (e.g., a web server and a web application server, a web application server and a database server, etc.). The key difference between the two forms of dependencies is that when one component **Uses** another, problems with the latter component can actually result in problems with the former component. With the **Connects** dependency, there are no such cause-effect relationships between the two components. To set the topology, choose the **Topology** option from the **Infrastructure** menu. This results in the display of currently configured segments (if any). If no segments pre-exist, then a message to the effect will be displayed (see Figure 2.17). The component topology comprises of one or more segments. A segment is a logical entity that represents a collection of components and the interdependencies between them. Segments can be chosen to represent user groups, organizational domains, or physical locations in the target environment. For example, the topology of a banking environment may include two segments – one representing all the component in the bank's NY branch and

Administering eG Enterprise

another representing the bank's CA branch. A new segment can be added by using the **Add New Segment** button available at the top. When this is done, the screen depicted by Figure 2.18 will appear wherein the name of the segment needs to be specified. Let us name the new segment as "demo_seg".

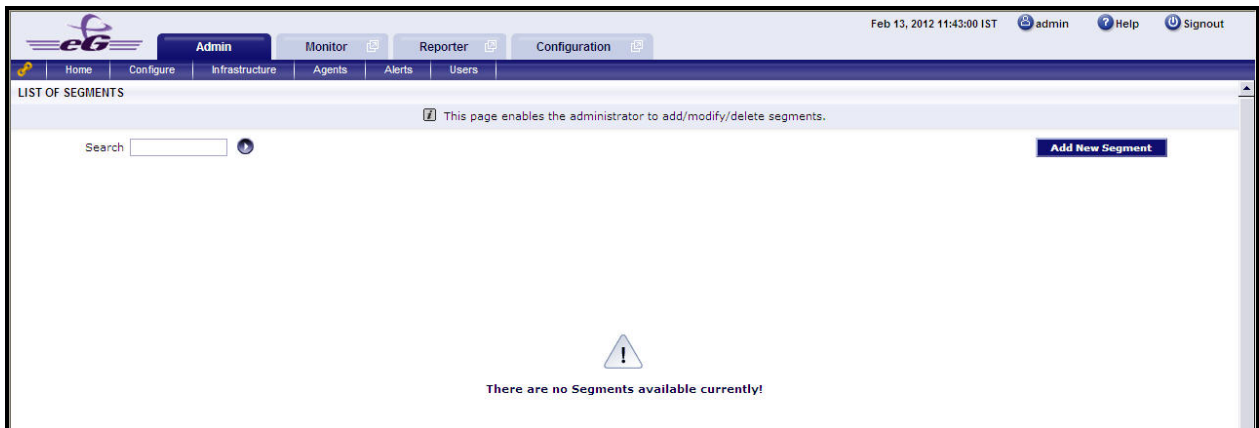


Figure 2.17: Screen displaying an existing segment

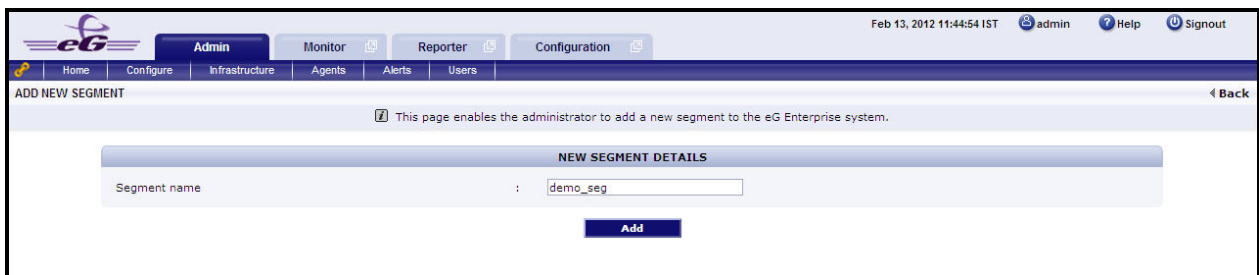


Figure 2.18: Specifying the details of a new segment

16. An infrastructure component can be associated with one or more segments. When configuring the topology of a segment, all the components not associated with any other segment are candidates for inclusion in the current segment. The interconnections between the components of a segment must be configured from left-to-right, with the left most node(s) representing the entry points through which users access the web services offered in the target environment.
17. For a simple environment like our target environment, a single segment would suffice. All the dependencies within our target environment can hence be defined under this segment.
18. Therefore, proceed to click the **Add** button in Figure 2.18 above, to invoke the screen depicted by Figure 2.19. For configuring our *demo_seg* segment, first choose the **Network node** option from the **Types of components** list box. The network node that we just added will appear in the **EXISTING COMPONENTS** box. Choose the newly added network node from the available options and then click the **Start** button. All the other managed components in the environment will appear in **ALL COMPONENTS** box. Now, select the IIS web server 192.168.10.59:7077 and click the **Connects >>** button. This establishes the connection between the network node and the IIS web server.
19. Next from the **Types of components** list box, select **IIS Web**. The IIS web servers that are managed currently by eG Enterprise appear in the **EXISTING COMPONENTS** box. Select the IIS web server 192.168.10.59:7077 and then click the **Start** button at the bottom. From the **ALL COMPONENTS** box, select the Tomcat server 192.168.10.59:8080, and click the **Uses >>** button. This indicates that the IIS web server uses the Tomcat server for processing the business logic components. Next, select

Administering eG Enterprise

Tomcat from the **Types of components** list box, and click the **Start** button. From the **ALL COMPONENTS** list, select the **Microsoft SQL 192.168.10.53:1433**, and click the **Uses >>** button to set the interdependency between the MS Sql server and the Tomcat server. The topology has now been configured and the preview of the topology configured is available in the **SEGMENT PREVIEW** section (see Figure 2.19).

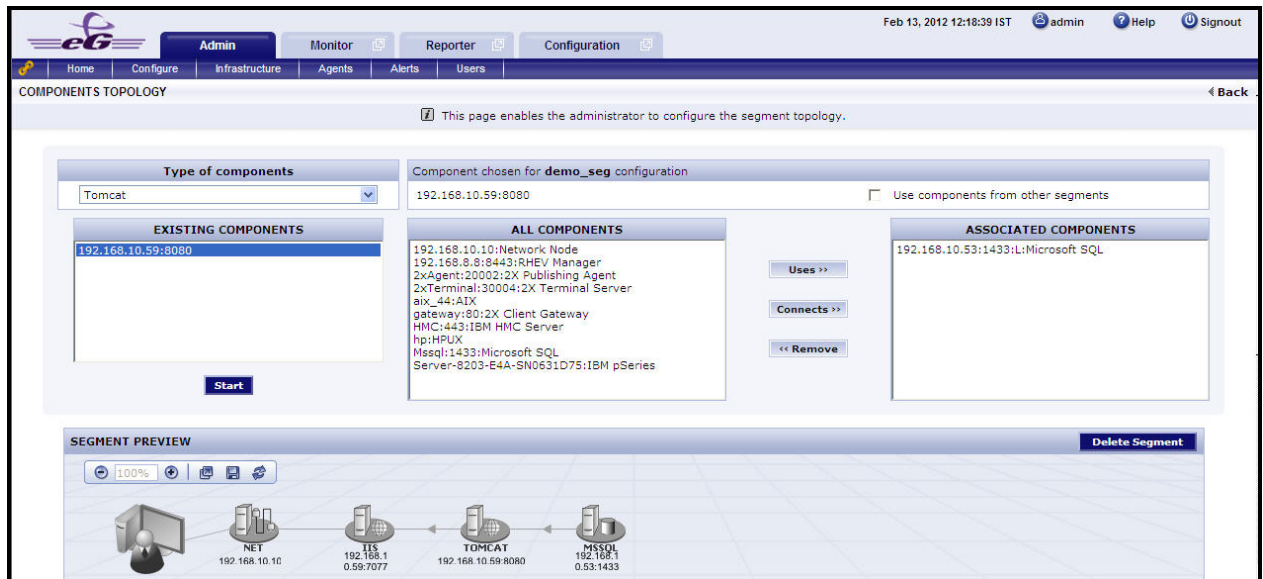


Figure 2.19: Configuring the segment topology

20. If you want to focus on the links emerging from or leading to a particular component in the topology, all you need to do is to move your mouse pointer over that component.
21. Moreover, in order to help you view and analyze the configured topology better, the **SEGMENT PREVIEW** section (see Figure 2.19) provides a special toolbar comprising of a wide variety of viewing options. This toolbar is also available while previewing the segment/service topology in the eG monitor interface.

Note:

The special toolbar will be available only if your browser supports the Java plugin Sun JRE 1.3.x and above. In case of browsers that do not support this plugin, the toolbar options are still available, but in the form of a shortcut menu that appears upon right-clicking anywhere in the **SEGMENT PREVIEW** section.

For a detailed description of each of the buttons in the toolbar, refer to the *eG User Manual*.

Note:

If you want to configure a segment with components that are already a part of other segments, then, while creating such a segment, ensure that the **Use components from other segments** check box in Figure 2.18 is selected. This check box is deselected by default, indicating that, by default, the **EXISTING COMPONENTS** and **ALL COMPONENTS** lists in Figure 2.18 display only those components that are not part of any other segment. By selecting the check box, you can make sure that components that belong to other segments are also available for inclusion in the new segment.

2.3.2 Configuring Services

The topology configured deals only with the flow of data across servers and not with services. The next step in administering eG Enterprise is to configure services. The different components working together deliver services to end users. The eG manager allows users to add one or more services for monitoring. A service can comprise just one or more independent components offering an end-user service (e.g., a web service offered by a web server).

Alternatively, a service can be a number of components working in conjunction. For example, a mobile payment service could involve a user accessing the service via an SMS gateway, which in turn hands off the request to a middleware application server. The application server could use a database for data storage / verification and rely on an external payment gateway. The collection of components and their interdependencies constitutes a service. Different business processes of an organization could be represented as a service. Note that a single segment topology can support multiple services and a single service may involve a subset of the components in a segment.

A service that can be associated only with a web server or a web application server is a web site. eG agents have the capability to monitor the performance of specific business functions supported by a web site. Such business function are called “transactions” in the eG Enterprise system.

For the target environment, we will configure one service, which is a web site.

1. To configure the service, first choose the **Topology** option from the **Services** sub-menu of the **Infrastructure** menu. Now, In the page that appears, click on the **ADD NEW SERVICE** button. The screen depicted by Figure 2.20 will appear.

The screenshot shows the eG Enterprise web interface. The top navigation bar includes 'Admin', 'Monitor', 'Reporter', and 'Configuration'. The 'Configuration' menu is expanded, showing 'Home', 'Configure', 'Infrastructure', 'Agents', 'Alerts', and 'Users'. The 'Configure' sub-menu is selected, and the 'ADD / MODIFY' option is chosen. The main content area is titled 'CONFIGURE - SERVICE >> ADD / MODIFY' and contains a form titled 'ADD NEW SERVICE'. The form has two fields: 'Name of the service' with the value 'demo_service' and 'Is this service a website' with a dropdown menu set to 'Yes'. An 'Add' button is at the bottom of the form.

Figure 2.20: Adding a new service

2. In the screen that appears, specify the **Name of the service** as *demo_service* in the text box provided. This name should be the same as the one used in the browser's command line to access the web site.

Administering eG Enterprise

- Then, from the **Is this service a website** list box, select **Yes**, so as to indicate that the new service is a web site.

Note:

While adding a service that is **not** a web site, the **No** option needs to be selected from the **Is this service a website** list box.

- Finally, click the **Add** button.
- Upon clicking, Figure 2.22 will appear, using which, the newly added web site is to be configured.

The screenshot displays the 'ADD NEW SITE' configuration interface in the eG Enterprise Admin console. The top navigation bar includes 'Admin', 'Monitor', 'Reporter', and 'Configuration'. The main form contains the following fields:

- Name of the site:** demo_service
- Alias name(s) for the site:** 192.168.10.59 (with a 'View' button)
- Segment(s) associated:** NONE
- Segment list:** demo_seg (dropdown menu)

Below the form, there are two panels:

- COMPONENTS UNDER NEW SITE:** Contains the entry '192.168.10.59:7077:IIS Web'.
- EXISTING COMPONENTS:** An empty box.

Between these panels are 'Remove >>' and '<< Add' buttons. An 'Update' button is located at the bottom center of the configuration area.

Figure 2.21: Configuring a web site

- The **Name of the site** box in Figure 2.21 will display the **Name of the service** specified earlier in Figure 2.20. The administrator can change it, if need be.

Note:

While adding a service that is **not** a website, the **Name of the site** text box of Figure 2.21 will be replaced by the **Name of the service** text box.

- A single site can be addressed by various other names in the environment (e.g., www.abc.com may also be accessed as www.abc.com:80, abc.com, us.abc.com, 172.169.10.20 etc.). These names (or IP address:port combinations) can be specified in the **Alias name(s) for the site** text box. This input field is optional. To ensure that all requests to a website are captured, it is essential to ensure that all the alias names for a site are specified accurately. The administrators can specify a maximum of six alias names, each of which should be comma separated. While multiple alias

names can be specified for a site, in the monitor interface, all the statistics pertaining to this web site will be reported using its site name that is specified in the **Name of the site** text box.

Note:

Alias names are applicable to web sites alone. Therefore, while configuring a service that is **not** a web site, the **Alias name(s) for the site** text box will not appear.

8. The **Segment list** box contains the list of fully configured segments in the target environment that contain atleast a single web or application server. The site can be associated with any of these segments. As our target environment consists of a single segment (*demo_seg*), select the same from this list. The **Independent_servers** option in this list box enables the administrator to associate a site to a single web or application server that does not form a part of the component topology.

Note:

In case of services that are **not** web sites, the **Segment list** list box will list all the fully configured segments in the target environment – not just the segments that contain web / application servers.

9. The **EXISTING COMPONENTS** box lists the web servers that can be associated with the web site being configured. Select the IIS web server 192.168.10.59:7077 and click the **Add >>** button to associate this web server with the eG monitoring application.

Note:

Unlike web sites that can be associated only with web / application servers, services that are **not** web sites can be associated with any component in the selected segment, or any independent component.

10. Click the **Update** button. The screen depicting the topology of the *demo_service* will appear as in Figure 2.23. While configuring the server topology, we had associated a network node, a Tomcat server, and a database server with this web server. These three components appear in the **ASSOCIATED COMPONENTS** box. Click **Update** to accept this site topology.

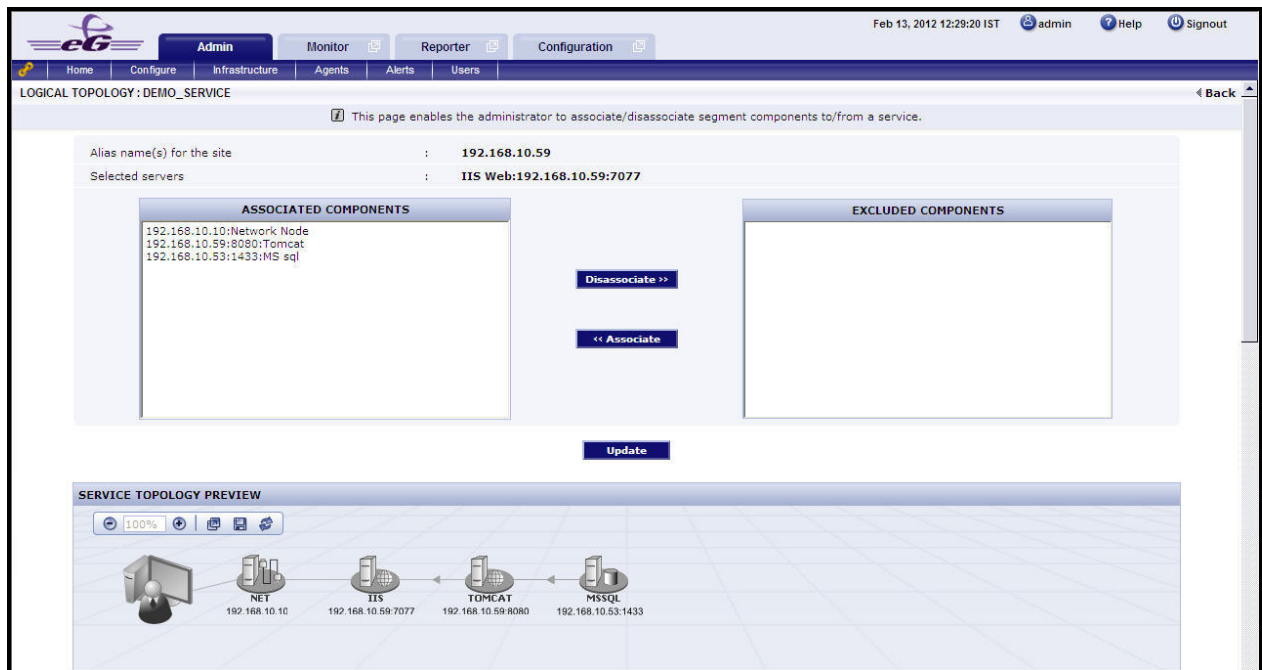


Figure 2.22: Site topology of demo_service

Note:

Once a segment is assigned to a service, then the **CONFIGURE SEGMENT** page of that segment will change to display a segment-service mapping at the bottom - i.e., the page will display a comma-separated list of services that are associated with the segment. To view/modify the service configuration directly from the **CONFIGURE SEGMENT** page, click on the corresponding service name in the mapping. The **ADD NEW SERVICE** page of that service will then appear.

- For each web site that has been configured, eG Enterprise has the ability to monitor individual transactions that happen via the site. To define the transactions to be monitored for the web site *demo_service*, choose the **Transactions** menu option from the **Services** sub-menu of the **Infrastructure** menu. The screen depicted by Figure 2.23 will appear. The sites that we just configured are displayed. The *demo_service* site can be associated with three main transactions, namely, *Upload*, *Login*, and *Images*. Let us now proceed to configure these transactions. Click the **Add / Delete Transaction** button in Figure 2.23. The screen depicted by Figure 2.25 will appear.

Note:

Transactions can be configured for web sites only. Therefore, Figure 2.23 will not list the services that are not websites.

Administering eG Enterprise

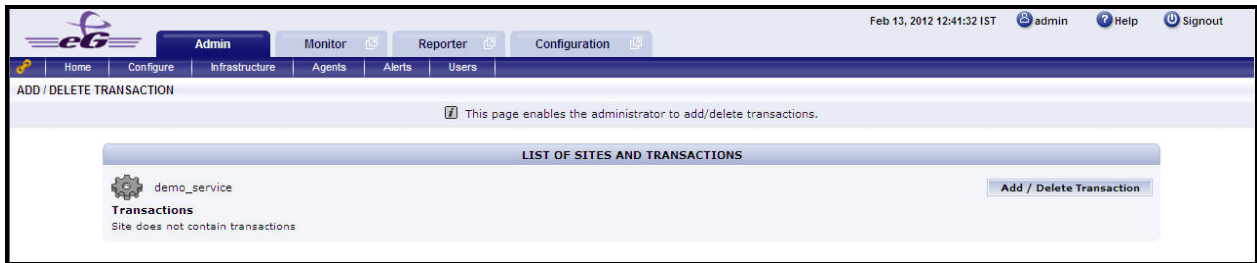


Figure 2.23: Configuring transactions

12. In Figure 2.24, the name of the transaction "*upload*" has to be specified in the **Transaction Name** text box. The pages to be associated with this transaction (**upload**) should be given in the **Pages to be Included** text box. Select an image to be associated with the current transaction from the list of options available. In this case, the image **Data transfer** has been associated with the new transaction. Finally, click the **Add** button to add this transaction. Follow the same procedure to configure the *Images* transaction. Remember to include the pages */*.gif,*.jpeg* to the transaction, and associate the **Images** image with it (see Figure 2.25). Similarly, add the *Login* transaction by including the page **/jsps/Loginform.jsp*, and associating the **Login** image (see Figure 2.26).

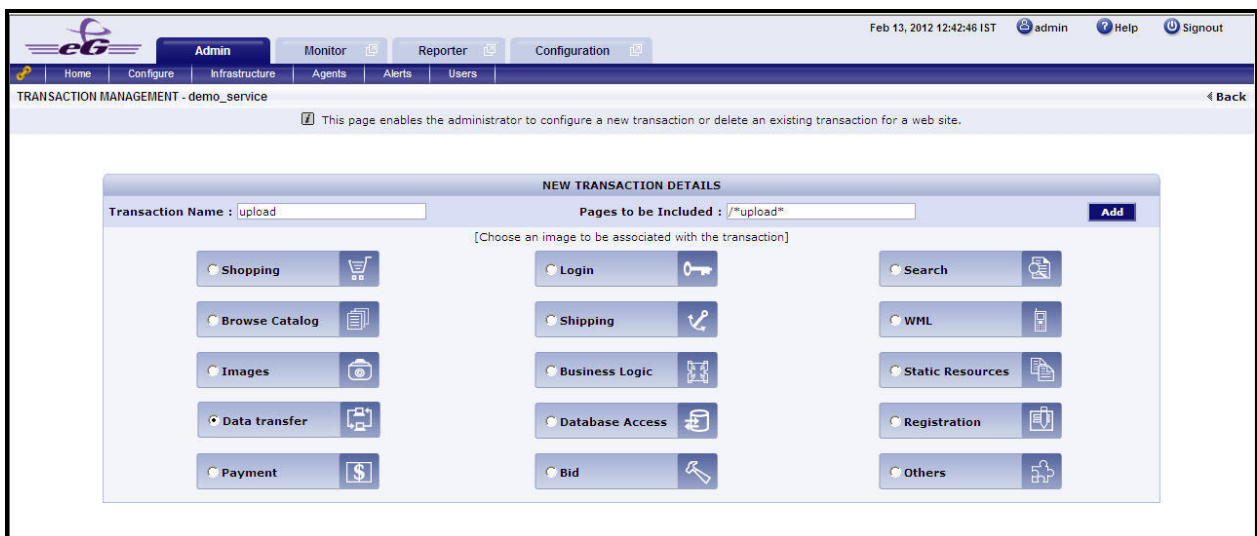


Figure 2.24: Configuring the *upload* transaction for the site *demo_service*

Administering eG Enterprise

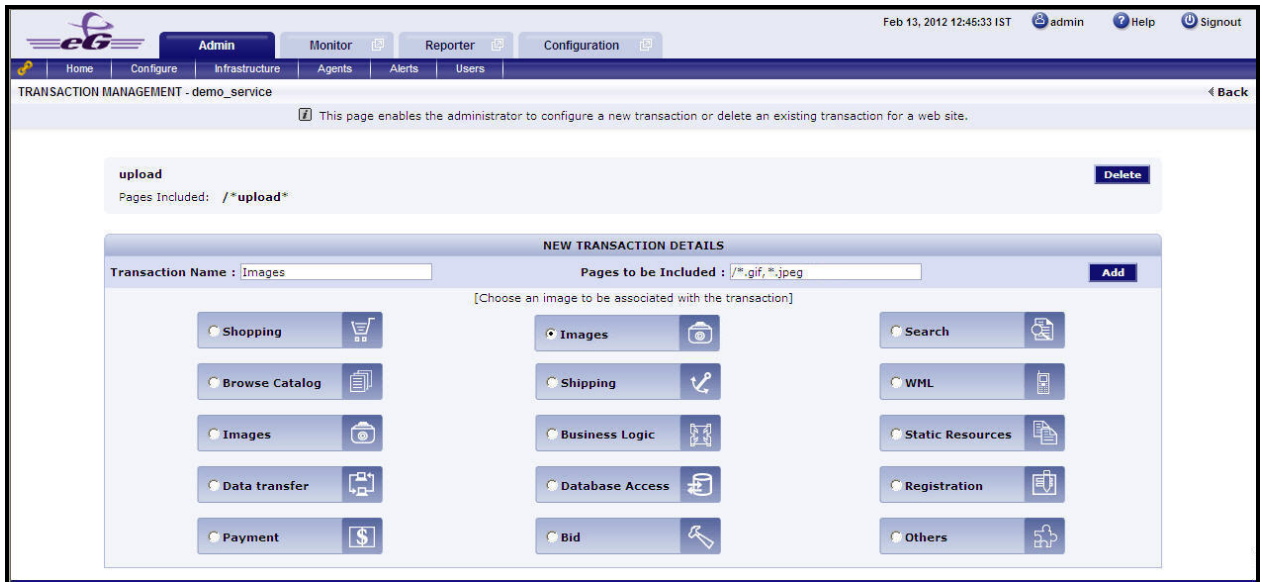


Figure 2.25: Configuring the *Images* transaction for the site *demo_service*

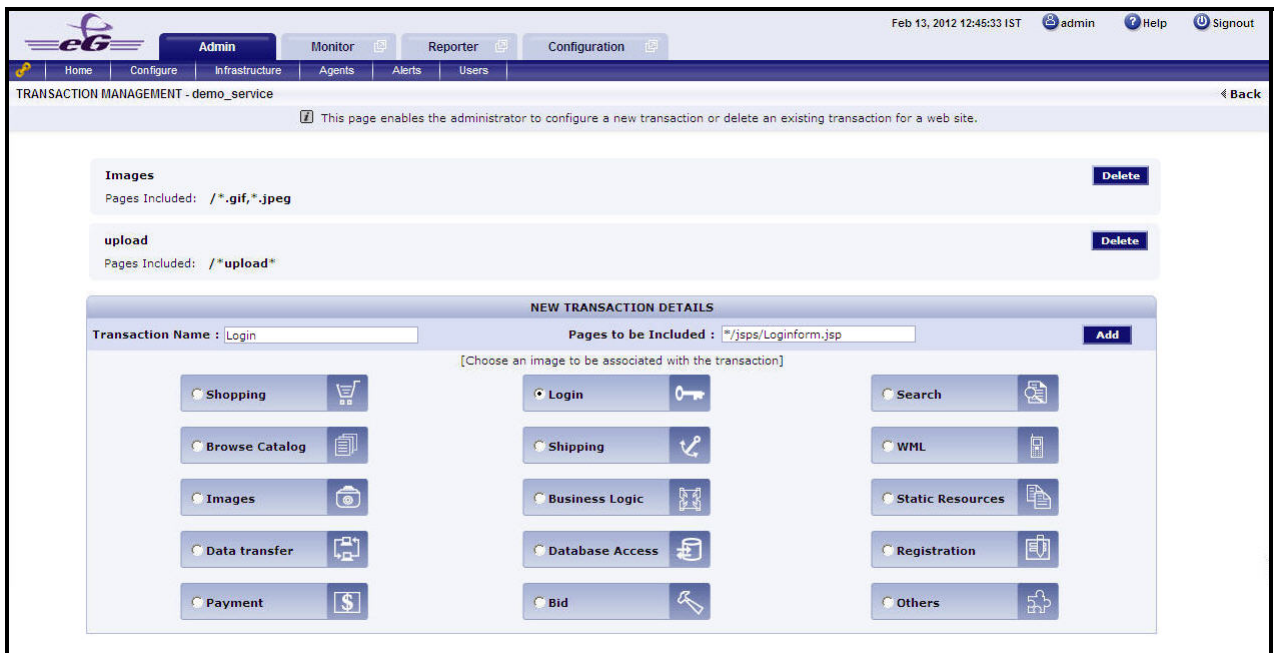


Figure 2.26: All configured transactions are being displayed

Note:

While mentioning the **Pages to be Included**, ensure that the page names should be prefixed by an * (asterisk) or a slash (/). If not, no measurements will be gathered from such pages.

2.3.3 Adding New Users

By default, eG Enterprise supports two users – one called *admin* (with a default password *admin*) who is by default assigned the **Admin** role, and another called *supermonitor* (with a default password *supermonitor*) who is by default assigned the **Supermonitor** role. Additional users can be created using the **Add User** option from the **Users** menu of the administrative interface, and a **User role** can be assigned to him/her that will clearly define their access rights. For each customer who has to be provided access to eG Enterprise, additional users can be created and roles assigned. Each user is associated with a virtual manager that is responsible for providing customized displays of the hosted environment.

Each user is optionally associated with a mail address where alarms will be forwarded. The user's profile also includes information regarding the customer's alarm preferences – whether alarms have to be forwarded in text or HTML mode, whether a complete list of alarms has to be generated each time a new alarm is added, or whether the new alarm alone should be sent via email, etc. Each user is associated with a subscription period. eG Enterprise allows the users to access the system until this period only. A *supermonitor* user takes an overall perspective of the hosted environment and this user account comes as default with eG Enterprise. This user has an unrestricted view of the target environment. He/she can receive alarms pertaining to the whole infrastructure that has been configured by the administrative user. Having completed configuring the components, topology, services, and transactions, let us proceed to add a **Monitor** user (*john*) and allocate specific services to him.

To achieve the above, do the following:

1. Select the **Add User** option from the **Users** menu of the eG administrative interface.
1. The **Users** menu allows the administrator to:
 - a. Add, modify or delete user roles
 - b. Add a new user
 - c. Delete an existing user
 - d. Add/Modify/delete Domains
 - e. Change the profile for any other user
 - f. Change the password of the administrator
 - g. View the information about user subscriptions for the eG service
2. Let us add the user *john* and allocate the *demo_service* site to him. For this, first click the **Add User** option. In the **ADD NEW USER** page (see Figure 2.27) that comes up, first select **Monitor** from the **User role** list box. Then, indicate whether the user being created is a **Local** user or a **Domain** user, by selecting the relevant option from **User authentication**. The eG administrative interface provides administrators with a wide variety of options to manage user information. Be it user creation, modification, deletion, or simply viewing user information, any type of user-related activity can be performed quickly and easily using the eG administrative console. Some target environments however, use the Active Directory server as the central repository for user information, and for authenticating domain logins. In such situations, if both the eG manager and the Active Directory consoles were to be used together for managing and validating the same set of users, it is bound to result in chaos! Therefore, to provide administrators with a single, central interface for efficiently managing users, eG Enterprise integrates seamlessly with the Active Directory server. The first step towards implementing this integration is the creation of a domain. Use the *Users -> Configure Domains* menu sequence to configure the domain, which is managed by the Active Directory (AD) server. Subsequent to domain creation, if you attempt to create a new user using this page, you will be prompted to indicate the **User authentication** mode that applies to the new user. If you are creating a domain user, whose requests are to be authenticated by the Active

Administering eG Enterprise

Directory, then select the **Domain** option. If you are creating a user who is local to the eG Enterprise system, and whose login requests are to be authenticated by the eG database, select the **Local** option. Since user *john* is a **Local** user, set the **User Authentication** mode to **Local**.

3. In the **User ID** text box, enter *john*. Provide the password for this user in the **Password** text box. Re-enter the same password in the **Retype password** text box.
4. Next, proceed to specify the subscription period for the user being added. For this, click on the Calendar button next to the **Expiry date** label. This will result in the display of a calendar from which you can choose the validity date for a new user. If the new user is to remain valid for an indefinite period, then click on the **No expiry** check box adjacent to the **Expiry date** text box. Doing so will no longer require the administrator to enter a specific date against the **Expiry date** field.
5. By choosing one or more of the check boxes corresponding to the **Alarms by mail/SMS** (see Figure 2.27), a user can indicate his/her preference in terms of the priority of problems for which he/she wishes to receive email alerts. For this scenario, select all the three options by enabling the check boxes beside them.
6. By default, eG Enterprise sends email alerts from the **Admin mail ID** configured in the **MAIL/SMS SETTINGS** page in the eG administrative interface. In MSP environments typically, different support groups are created to address performance issues relating to different customers. These support groups might prefer to receive problem intimation from customer-specific mail IDs instead of the global admin mail ID, so that they can instantly identify the customer environment that is experiencing problems currently. Moreover, this way, every support group will be enabled to send status updates on reported issues directly to the concerned customer, instead of overloading the admin mailbox. To facilitate this, the **MAIL/SMS SETTINGS** page allows the administrator to configure multiple **Mail sender IDs** - normally, one each for every customer in case of an MSP environment. Moreover, while creating a new user, the administrator can select one of these configured sender IDs from the **Mail sender** list and assign it to the new user, so that all email alerts received by the user are generated by the chosen ID only. Also, note that the **Admin mail ID** specified in the **MAIL/SMS SETTINGS** page will also be added to the **Mail sender** list in this page, and will be the default selection. For the purpose of our example, let us proceed with the default selection.

ADD NEW USER

This page enables the administrator to add a new user.

User role : Monitor

User authentication : ☐ Domain ☒ Local

User ID : john

Password : ****

Retype password : ****

Expiry date : ☒ No expiry

Alarms by mail / SMS : ☒ Critical ☒ Major ☒ Minor

Mail Sender : jeyakarthisa@eginnovations.com (Default)

Mail ID/Mobile number

To : john@czartech.com

Cc :

Bcc :

Command to be executed for alerts : [View](#)

Escalation mail ID/Mobile number :

Level 1 : bran@czartech.com

Level 2 : james@czartech.com

Type of notification : ☒ New ☐ Complete List

Message mode : ☒ Html ☐ Text

Include measure details in mail alerts : No

Include detailed diagnosis in mail alerts : ☐ Yes ☒ No

Time Zone : Asia/Calcutta (Default)

Email alerts only during shift periods : ☐ Yes ☒ No

Execute alerts only during shift periods : ☐ Yes ☒ No

SMS alerts only during shift periods : ☐ Yes ☒ No

Escalation alerts only during shift periods : ☐ Yes ☒ No

Alarm display : ☒ Critical ☒ Major ☒ Minor

Remote control : ☐ Enable ☒ Disable

Allow alarm deletion : ☐ Yes ☒ No

Allow alarm acknowledgement : ☐ Yes ☒ No

Monitor home page : Monitor Dashboard

Maximum timeline for reports : 2 weeks

[Next](#)

Figure 2.27: Adding a new user

- The eG manager is capable of alerting users as and when problems occur. The alarms are classified into critical, major, and minor. Enter the mail ID(s) to be associated with this user in the **Mail ID / Mobile Number** text box. It is to this ID(s) or mobile number(s) that the eG manager will send an alarm if an alarm situation arises. Multiple mail ids or mobile numbers can be specified as a comma separated list. When multiple mail IDs are specified, an administrator can specify which mail address(es) need to be in the **To:** field of the mail alarm and which ones should be in the **Cc:** and **Bcc:** fields.
- Like email IDs / mobile numbers, you can associate one/more custom scripts with users to the eG Enterprise system. Whenever alarms are raised/modified/closed for a specific user, the associated custom script will automatically execute, so that the details of the alarms are routed to third-party customer relationship management systems or TT systems, and trouble tickets automatically

created (or closed, as the case may be) for the corresponding user. The custom scripts thus provide a mechanism by means of which eG alerts are integrated into CRM/TT systems. These custom scripts can be configured in addition to or instead of email / SMS alerts. To associate the command that executes the custom script with a specific user's profile, specify the command in the **Command to be executed for alerts** text box of Figure 2.27.

Note:

The **Command to be executed for alerts** text box will appear only if the **Enable Command Execution** flag in the **COMMAND EXECUTION** section of the **MANAGER SETTINGS** page (Configure -> Manager Settings) is set to **Yes**.

9. The eG Enterprise system can also be configured to automatically escalate persistent problems to the next managerial level, so that the higher authority can initiate immediate action. When a user who receives an email/SMS alert of an issue is unable to resolve the reported issue for a pre-configured period of time, then the eG Enterprise system immediately forwards the email/SMS alert to a comma-separated list of mail IDs/mobile numbers specified against the **Level 1** field in the **Escalation mail ID/Mobile Number** section (see Figure 2.27). You can, if you so desire, define additional support levels by clicking on the '+' sign that appears at the end of the **Level 1** text box. This way, issues that remain unresolved even at **Level 1** will be escalated to **Level 2** and so on. A maximum of 5 levels can be added. To delete a newly added level, click on the '-' sign at the end of the corresponding **Level** text box.

Note:

Alarm escalation will work only if you configure the following:

- The duration beyond which the eG Enterprise system needs to escalate a problem to the next level
- The alarm priorities to be escalated

Both these parameters can be configured using the **ALARM ESCALATION** section in the **MAIL ALERT PREFERENCES** page that appears when the menu sequence *Alerts -> Mail Setings -> Alerts* is followed. To know more about the **MAIL ALERT PREFERENCES** page, refer to the *eG User Manual*.

10. A mail message is generated when new alarms are created or an existing alarm goes off, as the problem has been fixed. By choosing the **New** option corresponding to the **Type of notification** field, a user can indicate to eG Enterprise that when alerting the user via email, the system should send the details of newly added alarms only. If the **Complete List** option is chosen, the user will receive a complete list of current alarms. For now, choose the **New** option.
11. The **Message mode** option governs the format in which an alarm is reported in an email message. If the **Html** option is chosen, the alarm details are formatted as HTML text whereas the **Text** option formats the alarm details as plain text. Choose the **Html** option.
12. By default, the **No** option is chosen from the **Include measure details in alerts** list, indicating that the email alerts to a user will not include any measure details. However, if you want the email alerts to a user to include a time-of-day graph of the problem measure plotted for the last 1 hour (by default), then, pick the **Graph** option from this list. If you want the email alerts to a user to include the data plotted in a 1-hour measure graph, then, pick the **Data** option from this list.

13. By default, this flag is set to **No**. This implies that, by default, the detailed diagnosis (if available) of the problem measure will not be sent along with the email alerts to users. If you want the email alerts to a specific user to include detailed diagnosis information as well, then, set the **Include detailed diagnosis** flag to **Yes**. This information will enable users to move closer to the root-cause of the problem condition.
14. By default, all alerts generated by the eG Enterprise system are based on the eG manager's time settings. However, in an infrastructure that spans multiple geographies, users who are responsible for the proper functioning of servers in a particular geography (or time zone) may want to receive email alerts pertaining to those servers in their local time zone. To ensure this, you now have the option of configuring a time zone for a new user. The **Time Zone** list in Figure 2.27 displays a wide variety of time zones to choose from. By default, the manager's time zone is displayed here, indicating that, by default, email alerts are generated based on the manager's time settings. However, in case of target environments that are spread across multiple time zones, you may want to associate a different **Time Zone** with every user, so that email alerts sent to a user report problems based on that user's time settings, and not the manager's. In such a case, select the required **Time Zone** from the list. Once such a user is created, all subsequent email alerts that the user receives will report problems based on that user's **Time Zone** settings only.

Note:

While configuring a time zone, remember the following:

- The **Time Zone** specification in Figure 2.27 above applies only to **email alerts** and **not SMS alerts**.
- When normal mails are generated by the eG manager, the **Start Time** displayed in such mails will also be based on the **Time Zone** setting for the corresponding user.
- If a user is configured to use multiple email IDs (i.e., a comma-separated list of mail IDs has been provided in the **To**, **Cc**, and/or **Bcc** columns), then the **Time Zone** specification for that user applies to all the configured email IDs. In other words, every user can have a separate **Time Zone**, but every mail ID configured for a user cannot have a separate **Time Zone**.
- When mail alerts are being escalated, the time zone settings will be derived from the user account that the alarms pertain to. In other words, each escalation level will **NOT** have a separate **Time Zone** – the time zone setting for the user account will apply to escalated mails as well.
- Any alerts generated by the eG manager to report an unusual situation with the eG manager itself (e.g., database not working, agent not running, etc.) will not be affected by this **Time Zone** settings. All such alerts will be generated in the eG manager's local time zone setting.
- **Time Zone** changes made on the primary manager will be reflected on the secondary manager as well.

15. Some environments - especially the ones that span geographies - could have operators working in shifts; for instance, an MSP environment could comprise of one/more user groups, which might work only in the nights, in order to provide help-desk services to the customers in a particular

geographic region. These users naturally, would want to receive email alerts of issues only during their working hours; during the rest of day, they may prefer to be alerted via SMS. To facilitate this, eG Enterprise allows you to configure shift periods for individual users. Separate shift periods can be configured for receiving email alerts, SMS alerts, and escalation mails

For instance, if you want to indicate on which days and at what times a user needs to receive **email alerts of issues**, then he/she should first enable the **Email alerts only during shift periods** flag, by setting it to **Yes**.

16. Similar to email alerts, SMS alerts can also be configured to be sent out only during specified time periods on specific days of the week. The first step towards this is to enable the **SMS alerts only during shift periods** flag by selecting the **Yes** option in the **ADD USER** page. Using the **Days** and **Shifts** fields that appear subsequently, you can configure one/more **Day-Shift** combinations. To know more about configuring the **Day-Shift** combinations, refer to the *eG User Manual*.
17. Like email and SMS alerts, the eG manager can be configured to send escalation mails/SMS' also at pre-defined days and time slots. To enable this capability, first, turn on the **Escalation alerts only during shift periods** flag by selecting the **Yes** option in the **ADD USER** page. As before, this will bring up the **Days** and **Shifts** fields, using which you can configure the days on which and the times at which alerts are to be escalated to the specified individuals. For a more detailed information on how to configure the **Day-Shift** combinations, refer to the *eG User Manual*.

Note:

By default, the **Email alerts only during shift periods**, **SMS alerts only during shift periods** and **Escalation alerts only during shift periods** flags will appear in the **ADD USER** page. However, in environments where shifts are not relevant, such flags are meaningless. You can therefore ensure that these flags do not appear in the **ADD USER** page by following the steps given below:

- Open the **MAIL ALERT PREFERENCES** page by following the menu sequence: Alerts -> Mail Settings -> Alerts.
- In the **SHIFT PERIOD CONFIGURATION** section of this page, set the **Allow shift period configuration** flag to **No**. By default, this flag is set to **Yes**.
- Finally, register the changes by clicking the **Update** button.

18. To indicate preference in terms of the priority of problems that need to be viewed by user *john* in the eG monitor interface, select all the check boxes corresponding to **Alarm display**.
19. Using the **Remote control** option, you can indicate whether the remote control capabilities are to be switched on for the new user. This capability, when enabled, allows monitor users to remotely manage and control servers from a web browser itself. By default, this capability will be **Disabled** for a new user. To enable this capability for a particular user, select the **Enable** option. Disable the remote control capability for user *john*
20. To allow the new user to delete alarms from the **CURRENT ALARMS** window in the eG monitor interface, select the **Yes** option from the **Allow alarm deletion** section. Let us not grant this privilege to user *john*. Therefore, set **Allow alarm deletion** to **No**.
21. By default, the **Monitor Dashboard** appears as the home page of the eG monitoring console - i.e., as soon as a user logs into the monitoring console, the **Monitor Dashboard** appears as the first page by default. eG Enterprise however, allows administrators to set any page they deem fit as the **Monitor**

Home Page for individual users to the eG monitoring console. This way, every user, upon logging into the eG monitor interface, is enabled to view straight up the information that interests him/her the most, thereby saving time and minimizing the mouse clicks that may be required to navigate to that information!

The **Monitor home page** preference is typically driven by the monitoring needs of specific users and the roles assigned to them. For instance, a service manager, who is responsible for minimizing/eliminating service outages, would want to know on login how all the critical services in the environment are performing currently, and which services are in an abnormal state. For this purpose, administrators may want to set the **Service List** as the home page of such users.

22. To deny user *john* the right to acknowledge alarms, set **Allow alarm acknowledgement** to **No**. By acknowledging an alarm, a user can indicate to other users that the issue raised by an alarm is being attended to. In fact, if need be, the user can even propose a course of action using this interface. In such a case, a user with Admin or Supermonitor privileges (roles) can edit the acknowledgement by providing their own comments/suggestions on the proposed action.
23. Typically, eG Enterprise permits multiple users to simultaneously access the eG Reporter console and generate a wide variety of reports spanning any timeline of their choice. While this imparted tremendous flexibility in report generation, when concurrent users generate reports for broad time periods, report generation could slow down a little. In order to avoid this, administrators can set the maximum timeline for which each user can generate reports, by selecting an option from the **Maximum timeline for reports** list in the **ADD NEW USER** page. By default, **1 month** will be selected here. This implies that the user being created can generate reports for a maximum timeline of **1 month** only, by default. The other options in this list are as follows: 1 day, 2 days, 3 days, 4 days, 5 days, 6 days, 1 week, 2 weeks, 3 weeks, and 4 weeks. Besides ensuring that unauthorized users are denied access to more historical information than necessary, this timeline restriction also greatly reduces the strain on the eG database.
24. eG Enterprise allows administrators to assign specific segments/services/components/zones to a new user for monitoring. If one/more other existing users share the same assignment, then you can automatically associate all the infrastructure elements chosen for one user with other users to the eG Enterprise system. To achieve this, first select the **Auto-associate segments/services/components/zones to other users** check box. Doing so invokes an **Available users** list from which you can select the users to whom the same set of segments/services/components/zones need to be assigned. Since no other user exists in our environment, the **Auto-associate segments/services/components/zones to other user** check box will not appear, as shown by Figure 2.26.

Note:

The **Auto-associate segments/services/components/zones to other users** option will appear only when the **User role** chosen allows access to **Limited** components in the monitored environment. If the role chosen allows **Complete** components access, this option will not appear.

25. Then, click the **Next** button in Figure 2.27 to proceed with the user configuration. Doing so invokes Figure 2.28.

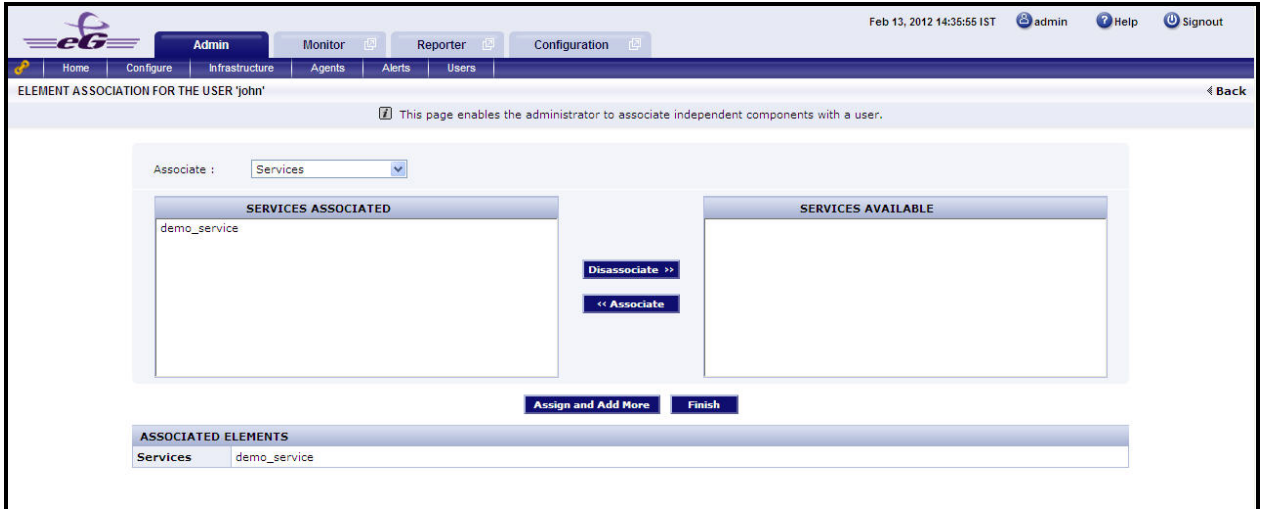


Figure 2.28: Configuring the services/segments/zones/components to be assigned to user *john*

26. Figure 2.28 appears only if the role assigned to a user allows **Limited** component access. Using Figure 2.28, you can assign specific services/service groups/segments/zones/components to a user for monitoring. For roles with **Complete** component access, this page will not appear. To know more about roles, please refer to the *eG User Manual*.

As the service *demo_service* needs to be assigned to user *john*, first select **Service** from the **Associate** list. The fully-configured services will then be listed in the **SERVICES AVAILABLE** list of Figure 2.27. Select the *demo_service* from this list and click the **Associate >>** button to transfer the selection to the **SERVICES ASSOCIATED** list. The **ASSOCIATED ELEMENTS** section of Figure 2.28 clearly indicates that the *demo_service* has been allocated to user *john*. If you want to add more infrastructure elements to the user, click the **Assign and Add More** button in Figure 2.28, and continue adding. If you are done with defining the monitoring purview of the user, then click the **Finish** button.

27. If the users wish to receive alarms through email, the mail server and the admin mail id details have to be specified in the page, which appears on choosing the **Server** option from the **Mail Settings** sub-menu of the **Alerts** menu.

2.3.4 Configuring Tests

For each server type, eG Enterprise has a set of predefined tests. While many of eG Enterprise tests do not require any manual configuration, some tests require explicit, manual configuration.

1. When a user attempts to sign out, the eG manager will prompt the user with a list of tests that have to be explicitly configured. Click the **Signout** option. Figure 2.29 depicts the list of tests that require manual configuration.

LIST OF UNCONFIGURED TESTS

This page enables the administrator to view unconfigured tests.

List of unconfigured tests for 'Microsoft SQL'

192.168.10.53:1433

Performance	Configuration	
SQL Applications	SQL Blocker Processes	SQL Database Space
SQL Database Status	SQL Engine	SQL Lock Waits
SQL Long Running Queries	SQL Network	SQL Open Cursors
SQL System Processes	SQL Transaction Logs	SQL User Processes

List of unconfigured tests for 'Mssql:1433'

Mssql:1433

Performance	Configuration	
SQL Applications	SQL Blocker Processes	SQL Database Space
SQL Database Status	SQL Engine	SQL Lock Waits
SQL Long Running Queries	SQL Network	SQL Open Cursors
SQL System Processes	SQL Transaction Logs	SQL User Processes

List of unconfigured tests for 'Tomcat'

192.168.10.59:8080

Performance	Configuration	
Tomcat Applications	Tomcat Cache	Tomcat Connectors
Tomcat JSPs	TomcatServlets	TomcatThreads
Java Classes	Java Server Web Access	JMX Connection to JVM
JVM CPU Usage	JVM File Descriptors	JVM Garbage Collections
JVM Memory Pool Garbage Collections	JVM Memory Usage	JVM Threads
JVM Uptime	Processes	

List of unconfigured tests for 'Network Node'

192.168.10.10

Performance	Configuration	
Device Uptime	Network Interfaces	

Figure 2.29: Tests that need to be configured

This page will also appear when the Agents -> Tests -> Configure -> Specific menu sequence is followed.

- To complete the configuration of the tests pertaining to the MS SQL server, choose one of the Sql server tests, say the SQL Network test, from Figure 2.29 by clicking on that. This action will take you to the page shown in Figure 2.30. When changing the configuration for specific servers, a "*" beside the text box corresponding to the parameter signifies that these values have to be manually configured by the user. The parameter values that require to be configured will typically be prefixed with a "\$" or contain a series of "*".

SQL Network parameters to be configured for 192.168.10.53 (Microsoft SQL)

192.168.10.53

TEST PERIOD	:	5 mins	
HOST	:	192.168.10.53	
PORT	:	1433	
INSTANCE	:	default	
* USER	:	sa	
* PASSWORD	:	*****	
* CONFIRM PASSWORD	:	*****	
SSL	:	☐ Yes ☒ No	
DOMAIN	:	none	
ISNTLMV2	:	☐ Yes ☒ No	<button>Validate</button>
DATABASE	:	master	
QUERY	:	SELECT * FROM master	<button>View</button>
ISPASSIVE	:	☐ Yes ☒ No	
APPLY TO OTHER COMPONENTS	:	☐	

Update

Figure 2.30: Configuring the SQL Network test

3. The parameters of the SQL Network test are:

- **TEST PERIOD** – How often should the test be executed
- **HOST** – The IP address of the Ms Sql server.
- **PORT** – The port number through which the MS SQL server communicates. The default port is 1433.
- **SSL** - If the MS SQL server being monitored is an SSL-enabled server, then set the **SSL** flag to **Yes**. If not, then set the **SSL** flag to **No**.
- **INSTANCE** - In this text box, enter the name of a specific MS SQL instance that is to be monitored. The default value of this parameter is "default". To monitor an MS SQL instance named "CFS", enter this as the value of the **INSTANCE** parameter.

Note:

If a particular instance name is provided here, ensure that the **PORT** parameter specification is **not modified**.

- **USER** – If an MS SQL server 7.0/2000 is monitored, then provide the name of a SQL user with the **Sysadmin** role. While monitoring an MS SQL server 2005/2008 on the other hand provide the name of a SQL user with the **CONNECT SQL**, **VIEW ANY DATABASE**, and **VIEW SERVER STATE** roles.
- **PASSWORD**- The password associated with the above user name (can be 'NULL'). Here, 'NULL' means that the user does not have any password.
- **CONFIRM PASSWORD** – Confirm the **PASSWORD** (if any) by retyping it here.
- **DOMAIN** - By default, *none* is displayed in the **DOMAIN** text box. If the 'SQL server and Windows' authentication has been enabled for the server being monitored, then the **DOMAIN** can continue to be *none*. On the other hand, if 'Windows only' authentication has been

enabled, then, in the **DOMAIN** text box, specify the Windows domain in which the managed MS SQL server exists. Also, in such a case, the **USER** name and **PASSWORD** that you provide should be that of a user authorized to access the monitored SQL server host.

- **DATABASE** - The name of the database to connect to. The default is "master". To monitor multiple databases, ensure that the database names are provided as a colon-separated list. Alternatively, you can use the semi-colon as the separator for the database names.
- **QUERY** - The select query to execute. The default is "select * from master.dbo.spt_monitor". Figure 2.30 displays a **VIEW** button next to the **QUERY** text box. Clicking on this button will open a pop-up window (see Figure 2.31) that will enable you to view the complete query and to make changes to it (if required) easily. Changes so made can be effected by clicking on the **APPLY** button in Figure 2.31. If the target MS SQL database server is installed as case sensitive, then the value of query parameter must be case sensitive. If multiple databases are specified in the **DATABASE** text box, then you will have to provide multiple queries here separated by a semi-colon (;) - for eg., *select * from master.dbo.spt_monitor;select * from alarm*. Every **DATABASE** being monitored, should have a corresponding **QUERY** specification.
- **ISNTLMV2** - In some Windows networks, **NTLM (NT LAN Manager)** may be enabled. NTLM is a suite of Microsoft security protocols that provides authentication, integrity, and confidentiality to users. NTLM version 2 ("NTLMv2") was concocted to address the security issues present in NTLM. By default, the **ISNTLMV2** flag is set to **No**, indicating that NTLMv2 is not enabled by default on the target Microsoft SQL host. Set this flag to **Yes** if NTLMv2 is enabled on the target host.

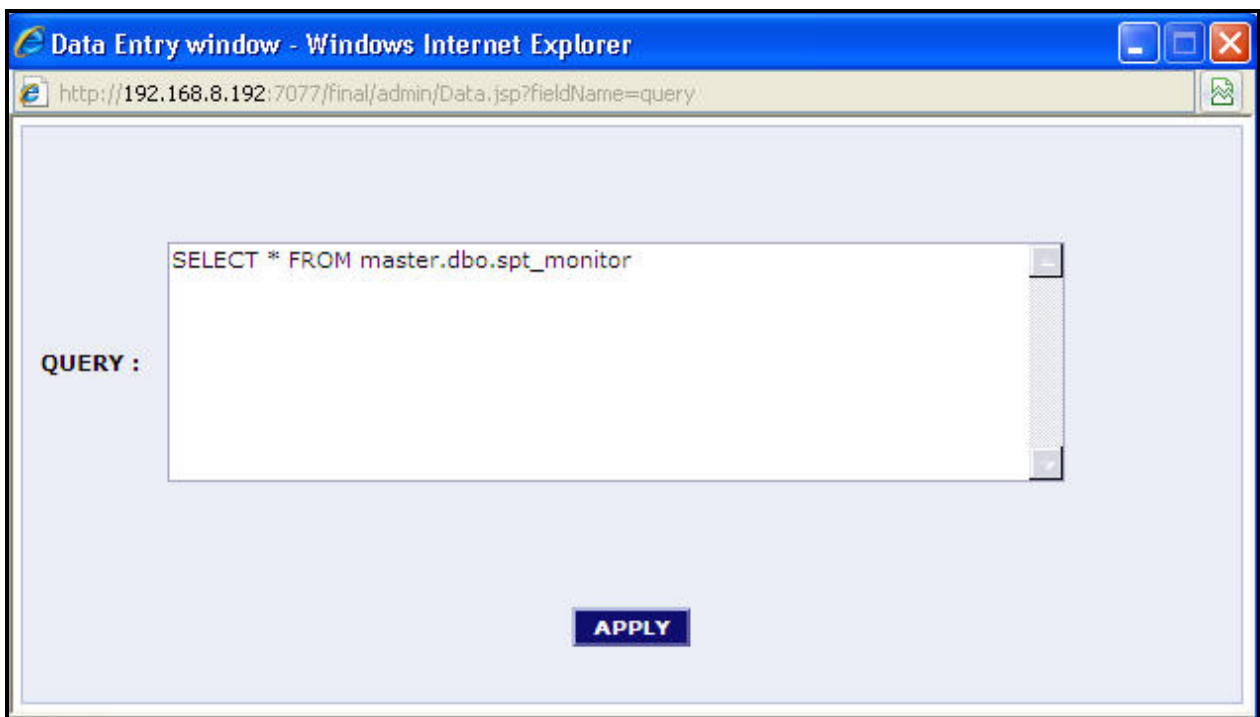


Figure 2.31: The VIEW window

- **ISPASSIVE** - If the value chosen is **Yes**, then the MS SQL server under consideration is a passive server in a SQL cluster. No alerts will be generated if the server is not running. Measures will be reported as "Not applicable" by the agent if the server is not up

Administering eG Enterprise

4. After providing the above-mentioned information, click on the **Update** button in Figure 2.30 to register the changes.
5. Now, try signing out again. The **LIST OF UNCONFIGURED TESTS** will reappear, but this time, the SQL Network test entry will not be present therein as it has already been configured. Now, click on the SQL Database Space test entry to configure it. Figure 2.32 lists the parameters of the SQL Database Space test for the Microsoft SQL server in our target environment.

SQL Database Space parameters to be configured for 192.168.10.53:1433 (Microsoft SQL)

192.168.10.53

TEST PERIOD	:	30 mins
HOST	:	192.168.10.53
PORT	:	1433
INSTANCE	:	default
SSL	:	☐ Yes ☒ No
* USER	:	sa
* PASSWORD	:	*****
* CONFIRM PASSWORD	:	*****
DOMAIN	:	none
ISNTLMV2	:	☐ Yes ☒ No Validate
EXCLUDEDDB	:	tempdb
ISPASSIVE	:	☐ Yes ☒ No
APPLY TO OTHER COMPONENTS	:	☐

Update

Figure 2.32: Configuring the SQL Database Space Test

6. Here again, specify the **USER** name and **PASSWORD** of a Microsoft SQL database user with the "Sysadmin" role (see Figure 2.32). Also, specify a comma-separated list of databases for which the space computation need not be done, against **EXCLUDEDDB**. The default value is 'tempdb'. Additionally, remember that frequent execution of this test could cause the Microsoft SQL server to incur high operational overheads, especially when the load on the server is very high. Accordingly, the **TEST PERIOD** is by default set to 30 minutes (see Figure 2.32). To register the changes, click on the **Update** button in Figure 2.32.
7. Attempting to signout now will bring up the **LIST OF UNCONFIGURED TESTS** (see Figure 2.29) once again, but this time, it will list the unconfigured tests for the Tomcat server and the network node alone. First, click on the Java Server Web Access test of the Tomcat server 192.168.10.59:8080 to configure it (see Figure 2.33).

Java Server Web Access parameters to be configured for 192.168.10.59:8080 (Tomcat)

192.168.10.59

TEST PERIOD	:	5 mins
HOST	:	192.168.10.59
PORT	:	8080
* EGURI	:	http://192.168.10.59:7

Update

Figure 2.33: Configuring the Java Server Web Access test

8. In Figure 2.33, the **EGURI** parameter requires configuration. The Java Server Web Access Test makes use of a file named **EgPerfTest.jsp** to generate measures. By default, this file is located in the

<EG_INSTALL_DIR>/lib directory. To execute the Java Server Web Access test, move this file to one of the application directories of the Orion/Tomcat server. While configuring the Java Server Web Access test, specify the location of the application directory where the **EgPerfTest.jsp** file resides, in the **EGURI** text box, in the following format: <http://<Ipaddress:portNo/directory name>>. Once the location is specified, commit the changes by clicking on the **Update** button in Figure 2.33.

9. Then, proceed to configure the JVM Memory Usage test for the Tomcat server being monitored. Figure 2.34 depicts the parameters of this test.

JVM Memory Usage parameters to be configured for 192.168.10.59 (Tomcat)	
TEST PERIOD	: 5 mins
HOST	: 192.168.10.59
PORT	: 8080
TIMEOUT	: 10
MODE	: ☐ SNMP ☒ JMX
* JMX REMOTE PORT	: 70
JNDI NAME	: jmxrmi
USER	: tomcat
PASSWORD	:
CONFIRM PASSWORD	:
HEAP ANALYSIS	: ☐ Yes ☒ No
DD FREQUENCY	: 1:1
DETAILED DIAGNOSIS	: ☒ On ☐ Off

Update

Figure 2.34: Configuring the JVM Memory Usage test

10. In Figure 2.34, specify the following:

- **TESTPERIOD** - How often should the test be executed
- **HOST** - The host for which the test is to be configured
- **PORT** - Mon The port number on which the Tomcat server listens
- **MODE** - This test can extract metrics from the Java application using either of the following mechanisms:
 - Using SNMP-based access to the Java runtime MIB statistics;
 - By contacting the Java runtime (JRE) of the application via JMX
- To configure the test to use SNMP, select the **SNMP** option. On the other hand, choose the **JMX** option to configure the test to use JMX instead. By default, the **JMX** option is chosen here.
- **JMX REMOTE PORT** - This parameter appears only if the **MODE** is set to **JMX**. Here, specify the port at which the **JMX** listens for requests from remote hosts. Ensure that you specify the same port that you configured in the *management.properties* file in the <JAVA_HOME>\jre\lib\management folder used by the target application.
- **USER**, **PASSWORD**, and **CONFIRM PASSWORD** - These parameters appear only if the **MODE** is set to **JMX**. If JMX requires **authentication only** (but no security), then ensure that the **USER** and **PASSWORD** parameters are configured with the credentials of a user with *read-write* access to JMX. To know how to create this user, refer to the *Monitoring Java Applications* document. Confirm the password by retyping it in the **CONFIRM PASSWORD** text box.

Administering eG Enterprise

- **JNDIName** – This parameter appears only if the **MODE** is set to **JMX**. The **JNDIName** is a lookup name for connecting to the JMX connector. By default, this is *jmxrmi*. If you have resregistered the JMX connector in the RMI registry using a different lookup name, then you can change this default value to reflect the same.
- **SNMPPort** – This parameter appears only if the **MODE** is set to **SNMP**. Here specify the port number through which the server exposes its SNMP MIB. Ensure that you specify the same port you configured in the *management.properties* file in the <JAVA_HOME>\jre\lib\management folder used by the target application (refer to the *Monitoring Java Applications* document for details).
- **SNMPVersion** – This parameter appears only if the **MODE** is set to **SNMP**. The default selection in the **SNMPVersion** list is **v1**. However, for this test to work, you have to select SNMP **v2** or **v3** from this list, depending upon which version of SNMP is in use in the target environment.
- **SNMPCommunity** – This parameter appears only if the **MODE** is set to **SNMP**. Here, specify the SNMP community name that the test uses to communicate with the mail server. The default is public. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVersion** chosen is **v3**, then this parameter will not appear.
- **Username** – This parameter appears only when **v3** is selected as the **SNMPVersion**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **Username** parameter.
- **AuthPass** – Specify the password that corresponds to the above-mentioned **Username**. This parameter once again appears only if the **SNMPVersion** selected is **v3**.
- **Confirm Password** – Confirm the **AuthPass** by retyping it here.
- **AuthType** – This parameter too appears only if **v3** is selected as the **SNMPVersion**. From the **AuthType** list box, choose the authentication algorithm using which SNMP v3 converts the specified **Username** and **Password** into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options:
 - **MD5** – Message Digest Algorithm
 - **SHA** – Secure Hash Algorithm
- **EncryptFlag** – This flag appears only when **v3** is selected as the **SNMPVersion**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **EncryptFlag** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option.
- **EncryptType** – If the **EncryptFlag** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **EncryptType** list. SNMP v3 supports the following encryption types:
 - **DES** – Data Encryption Standard
 - **AES** – Advanced Encryption Standard
- **EncryptPassword** – Specify the encryption password here.

Administering eG Enterprise

- **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here.
- **TIMEOUT** - This parameter appears only if the **MODE** is set to **SNMP**. Here, specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.
- **HEAP ANALYSIS** – By default, this flag is set to **off**. This implies that the test will not provide detailed diagnosis information for memory usage, by default. To trigger the collection of detailed measures, set this flag to **On**.
- **JAVA HOME** – This parameter appears only when the **HEAP ANALYSIS** flag is switched **On**. Here, provide the full path to the install directory of **JDK 1.6 or higher** on the application host. For example, *c:\JDK1.6.0*.**URL** - Specify the URL of the managed Tomcat web server to enable the test to connect to it and extract measures from it. The **URL** specification should be of the format: *http://{TomcatIP}:{TomcatPort}*.
- **DD FREQUENCY** - Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *1:1*. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against **DD FREQUENCY**.
- **DETAILED DIAGNOSIS** - To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option.

The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:

- The eG manager license should allow the detailed diagnosis capability
- Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.**USERNAME** – A valid user name to login to the Tomcat server to be monitored

11. Then, click the **Update** button in Figure 2.34 to register the changes.

12. Next, configure the Processes test for the Tomcat server by clicking on the Processes test listed in Figure 2.29. Figure 2.35 then appears.

Processes parameters to be configured for 192.168.10.59 (Tomcat)

192.168.10.59

TEST PERIOD	:	5 mins
HOST	:	192.168.10.59
PORT	:	8080
* PROCESS	:	Tomcat:tomcat.exe
WIDE	:	☒ Yes ☐ No
USEPS	:	☐ Yes ☒ No
USER	:	none
CORRECT	:	☐ Yes ☒ No

View

Update

Figure 2.35: Configuring the Processes test

Administering eG Enterprise

13. In the **PROCESS** text box of Figure 2.35, enter a comma separated list of names:pattern pairs which identify the process(es) associated with the server being considered. processName is a string that will be used for display purposes only. processPattern is an expression of the form - *expr* or expr or *expr or expr* or *expr1*expr2*... or expr1*expr2, etc. A leading '*' signifies any number of leading characters, while a trailing '*' signifies any number of trailing characters. For the Tomcat server in our target environment, let us monitor the Tomcat server executable *tomcat.exe*. Accordingly, the **PROCESS** parameter can be specified as *Tomcat:*tomcat.exe** (see Figure 2.35).
14. In addition to the **PROCESS** parameter, a **CORRECT** flag is also available (see Figure 2.35). eG Enterprise provides "ready-to-use" scripts to correct the most common problems with the ProcessTest and WinServiceTest. By default, this capability will be set to **No**. Let us not enable this capability for our example. Therefore, click on the **Update** button in Figure 2.35, to save the changes.
15. Finally, proceed to configure the Network Interfaces test of the network node 192.168.10.10:NULL (see Figure 2.36).

The screenshot shows a configuration window titled "Network Interfaces parameters to be configured for 192.168.10.10 (Network Node)". The window contains a table of configuration parameters for the network node 192.168.10.10. The parameters are as follows:

192.168.10.10	
TEST PERIOD	: 5 mins
HOST	: 192.168.10.10
SNMPPORT	: 161
TIMEOUT	: 10
SNMPVERSION	: v1
* SNMPCOMMUNITY	: public
USEEXTENSION	: ☐ Yes ☒ No
USEALIAS	: ☒ Yes ☐ No
DISCOVERBYSTATE	: ☒ Yes ☐ No
ONLYUP	: ☐ Yes ☒ No
SHOW ALIAS AND INTERFACE NAME	: ☐ Yes ☒ No
EXCLUDE	: Null0,Nu0
FULLDUPLEX	: ☒ Yes ☐ No
DD FREQUENCY	: 1:1
SHOWDETAILS	: Yes
DETAILED DIAGNOSIS	: ☒ On ☐ Off

At the bottom right of the configuration area, there is a blue "Update" button.

Figure 2.36: Configuring the Network Interfaces test

16. In Figure 2.36, the **SNMPCOMMUNITY** string for the network node has to be provided. The default value for the SNMP community string is "public". However, the value specific to the user environment has to be provided. After specifying the string, click the **Update** button to register the changes.
17. With that, we have completed configuring our target environment. Using the **Signout** option, log out of the administrative interface. As already mentioned, we need to install and configure agents on the database server. The following section briefs the steps involved in installing and configuring the eG agent.

Infrastructure Monitoring using eG Enterprise

This chapter will run you through the quick steps involved in monitoring the target environment that was configured in Chapter 2. The first step towards this is to install and configure the eG agents.

3.1 Installing and Configuring eG Agents

1. **Installing and Configuring an eG agent:** Agents are software components deployed at various points in the IT infrastructure system. Like the eG manager software, the eG agent setup software is provided as a self-extracting executable program called **eGAgent.exe** that can be installed and configured on the Windows environment. The eG agent software comes as a standard package called **eGAgent** for a Solaris environment, and for Linux, AIX, and Free BSD environments, it is given as a tar file called **eGAgent.tar**. The eG agent software for HP-UX is provided as a depot file by name **eGAgent.depot**. Installation of the eG agent requires administrator privileges of the local machine. Please look at Chapter 2 and 3 of the *eG Installation Guide* for an elaborate explanation on the steps involved in installing the eG agent. In the target environment, agents are deployed on 192.168.10.59, and 192.168.10.53, both of which are Windows systems. A default external agent has also been deployed on the eG manager host 192.168.10.63, which is also a Windows system.
2. **Configuring the eG web adapter capability:** The eG web adapter technology tracks individual transactions performed by users of a web site in real-time without the need for explicit, expensive logging. The web adapter forms a part of the eG agent package. When the agent is configured, it is enabled to communicate with the web adapter to report statistics in real-time to the eG manager. The web adapter must be configured for each and every web server that must be monitored by eG. A user can configure the web adapter only for the web servers for which he/she has permissions to administer. To explicitly configure the eG web adapter capability in Solaris environments, run the command `/opt/egurkha/bin/setup_webadapter`. On Windows environments, the agent modification process prompts whether monitoring should be configured for an IIS web server. If the user chooses this option, the web adapter is configured to monitor the IIS web server. Chapter 3 of the *eG Installation Guide* provides more details of the web adapter.
3. **Starting the eG agent:** The next step after installing and configuring an eG agent is to start the agent. To start the agent, click the **START** button on the task bar of the Windows system. From thereon, select Programs > eG Monitoring Suite > eG Agent > Start Agent. In Unix environments, this is achieved by executing the command `/opt/egurkha/bin/start_agent`.

We can now login to eG Enterprise as a supermonitor or as one of the monitor users created using the eG admin interface to view and act on the various metrics reported by the eG agents.

3.2 Infrastructure Monitoring using eG Enterprise

As before, access the eG user interface using the URL `http://192.168.10.63:7077/` (or if the manager is SSL-enabled, then use `https://192.168.10.63:7077/`). The screen depicted by Figure 2.3 will appear. Let us first look into what a *supermonitor* user gets to view on the monitoring front. As already mentioned, eG Enterprise is preconfigured with a user account named *supermonitor* (with the default password *supermonitor*) that can be used to login. Specify this in the appropriate space provided and then click the **AUTHENTICATE** button. An alarm window stating that there are no alarms in the environment will first appear when the *supermonitor* comes in for the first time.

Behind the **ALARMS** window is the **MONITOR HOME** page (see Figure 3.1). If no alarms exist in the environment, then this is the first page that will be displayed in the monitor interface.

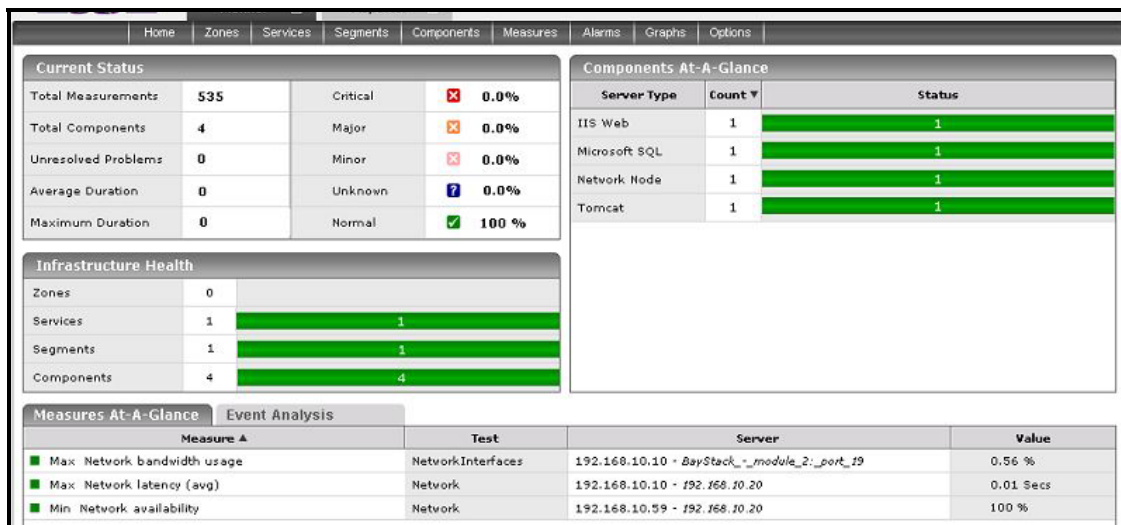


Figure 3.1: The Monitor Home page

This page quickly updates the monitor user with the health of the entire monitored environment. The page reveals the following information:

- The first section is the **Current Status** section that reveals at a glance, the status of the measurements reported to the eG manager. Besides displaying the total number of monitored components and the number of performance metrics collected by the eG agents from these components, this section also reveals the percentage of total measurements that are in the critical, major, minor, normal, and unknown states. Using this information, an accurate assessment of the overall infrastructure performance can be made (see Figure 3.1). You can click on any of the states in the **Current Status** section to view the current alarms of the corresponding priority.
- Next to the **Current Status** section is the **Infrastructure Health** section. This section takes the help of a bar graph to clearly indicate the number of zones, services, segments, and components that are in the Critical, Major, Minor, Normal, and/or Unknown states.

The table below explains the color-coding scheme adopted by eG for indicating the states of the components:

Infrastructure Monitoring using eG Enterprise

Color	State
Red	Critical
Orange	Major
Pink	Minor
Green	Normal
Blue	Unknown

Large infrastructures spanning geographies can pose quite a monitoring challenge owing to the number of components involved and their wide distribution. Administrators of such infrastructures might therefore prefer to monitor the infrastructure by viewing it as smaller, more manageable business units. In eG parlance, these business units are termed **ZONES**. A zone can typically comprise of individual components, segments, services, and/or other zones that require monitoring. For example, in the case of an infrastructure that is spread across the UK, USA, and Singapore, a zone named *USA* can be created consisting of all the components, segments, and services that are operating in the US branch alone. The *USA* zone can further contain an East-coast zone and a West-coast zone to represent infrastructure and services being supported on the two coasts of the US.

If one/more zones have been configured in an environment, then the **Infrastructure Health** section will display a **Zones** bar graph representing the number of zones and their state. However, as no zones have been configured for our example, the **Zones** bar graph is not available in Figure 3.2.

Moreover, since our example includes only one service, the **Services** bar graph indicates the same (see Figure 3.2). Clicking on a division in the bar graph will take you to a page that lists the services that are in a particular state (see Figure 3.2).

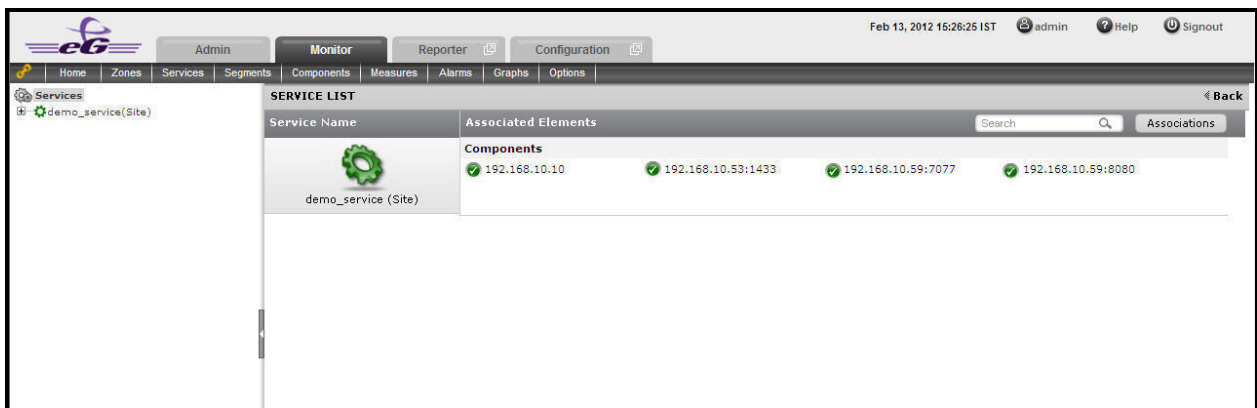


Figure 3.2: Viewing the list of services in a particular state

Our target environment comprises of only one service, which is the "*demo_service*" site. Figure 3.2 displays the *demo_service* site, which is currently, in the Normal state.

If you now click on the **Associations** button in Figure 3.2, Figure 3.3 will appear.

Infrastructure Monitoring using eG Enterprise

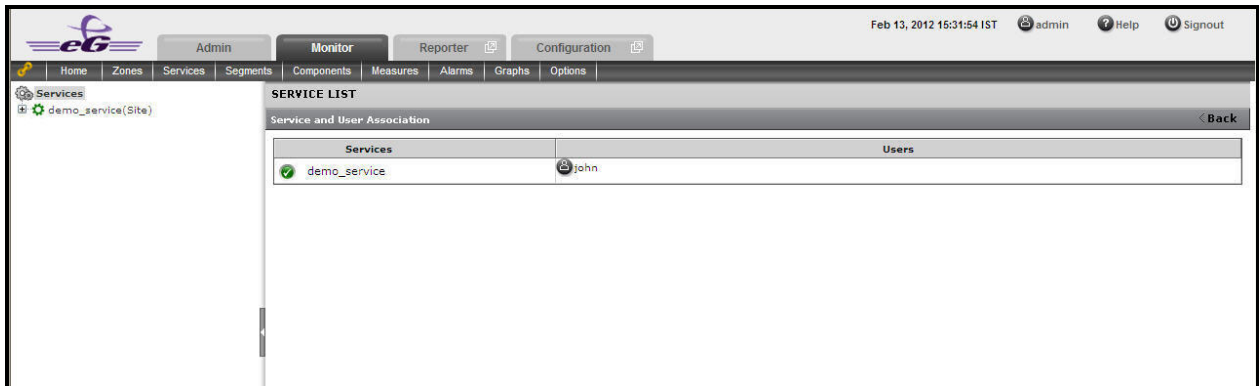


Figure 3.3: Viewing the user-service mappings

Figure 3.3 displays the complete list of services that have been configured for the environment, the state of the services, and the users associated with each of them. Clicking on a service in Figure 3.3 will reveal the transactions that have been configured for that service.

Let us now take a look at the **Segments** bar graph in Figure 3.1. This indicates that our infrastructure consists of only one fully-configured statement, which is currently in good health. To know which segment this is, click on the **Segments** bar graph. Figure 3.4 then appears, clearly indicating that *demo_seg* that we had previously configured is the segment that is in a Normal state.

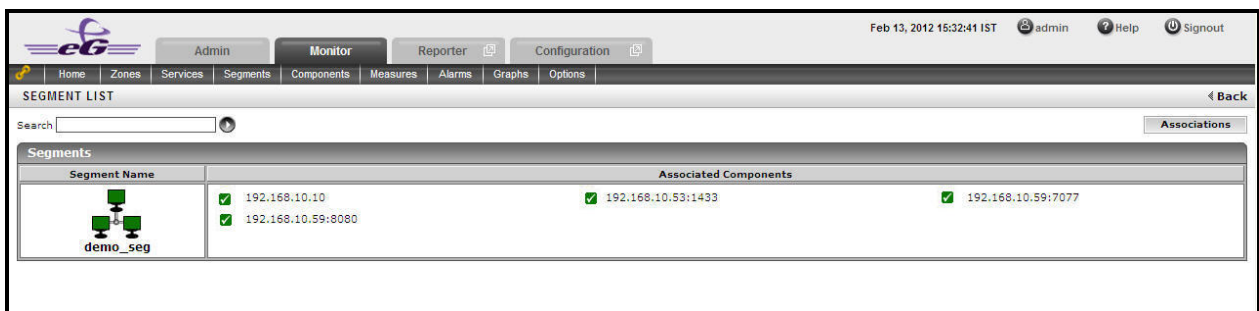


Figure 3.4: Viewing the segments in a Normal state

In the same way, the **Components** bar graph reveals the number and current status of the components managed in the target environment. According to Figure 3.1, our example consists of 4 components, all in the Normal state of activity. Typically, to view the list of components of a particular state, you will have to click on that division of the **Components** bar graph that corresponds to that state. Since all the monitored components in our example are in the Normal state currently, simply click on the **Components** bar graph. Figure 3.5 will then appear, listing the normal components.

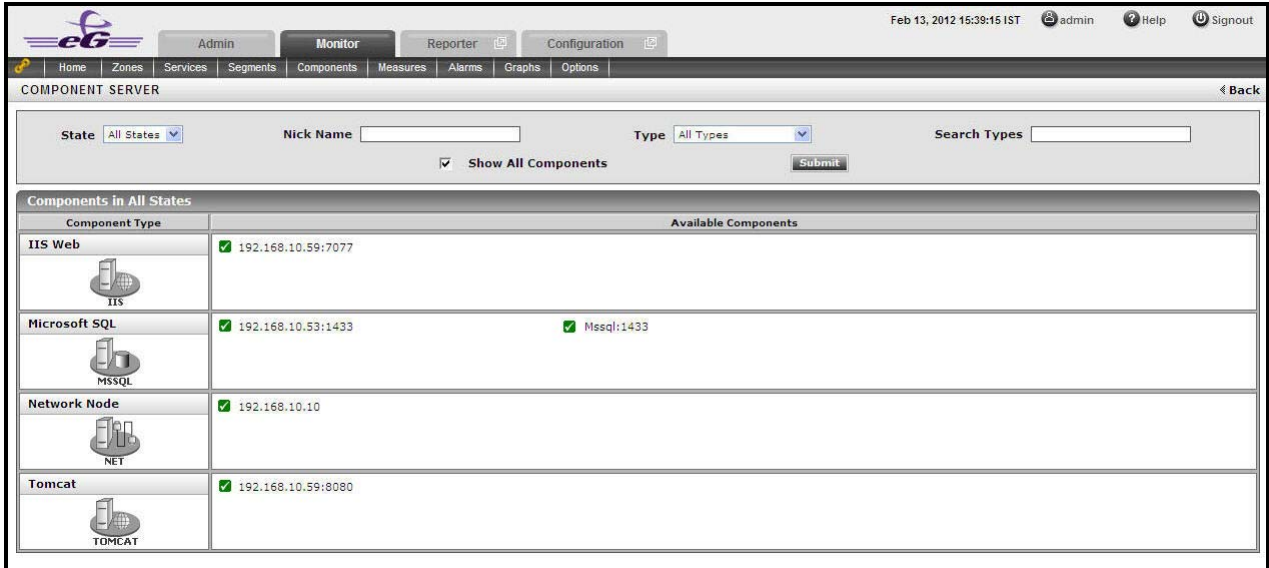


Figure 3.5: Viewing the list of components in a particular state

The IIS web server, MS SQL server, the network node, and the Tomcat server are the four components that are associated with our target environment. Figure 3.5 displays these components and their current state, which is Normal.

- Below the **Infrastructure Health** section you will find a **Measures At-A-Glance** section that provides the min/max values of critical measurements updated in real-time. By default, using this section, you can quickly find answers to the following critical performance queries:
 - (a) Which host across the environment is consuming the maximum CPU?
 - (b) Which host in the monitored infrastructure has very little free memory to its credit?
 - (c) Which disk partition on which host is utilized the maximum?
 - (d) Which is the web server that services the maximum number of requests over time?
 - (e) Which network interface is using up a lot of bandwidth?
 - (f) On which host are TCP retransmits very high?
 - (g) Where in the target environment is network latency the maximum?
 - (h) TCP connections to which port are taking too long?
 - (i) Which host is currently not available over the network?

You can however, change this default setting to reveal more or less - i.e., you can add to the measure list displayed here, or remove a few measures from the displayed list. To achieve this, do the following:

- Login to the eG administrative interface as *admin*.
- Go to the **MONITOR SETTINGS** page using the menu sequence, Configure -> Monitor Settings.
- Click on the **Measures At-A-Glance** button in the **MONITOR SETTINGS** page.
- The resulting **MEASURES AT-A-GLANCE CONFIGURATION** page will display the default measure configurations for the **Measures At-A-Glance** section. To know how to

manipulate the controls in the page to add more measures or remove a few of the pre-configured measures, refer to the *eG User Manual*.

The min/max values of the configured measures will then be displayed in the **Measures At-A-Glance** section. The first column of the **Measures At-A-Glance** section in Figure 3.1 indicates the current state of the measure (whether Normal/Critical/Major/Minor/Unknown). The **Measure** column is where the configured measures will be displayed. Similarly, each of the configured tests will appear in the **Test** column. Besides, a **Server** column exists, which displays the name of the component and the descriptor, which has currently registered the maximum/minimum value (as the case may be) for every chosen measure. Finally, the current value of the measures for the displayed components will be displayed in the **Value** column.

Using the information provided by the **Measures At-A-Glance** section, administrators can receive instant status updates on sensitive performance parameters, and can also accurately determine, at a glance, the component on which the parameter is currently experiencing issues (if any), thereby simplifying problem identification.

Clicking on the contents of any cell in this section, will lead you to the layer model of the corresponding component.

Optionally, you can even switch off the **Measures At-A-Glance** section. To do so, you will have to set the **Compute top metrics** parameter in the **MEASURES AT-A-GLANCE CONFIGURATION** page of the eG administrative interface to **No**. By default, this parameter is set to **Yes** indicating that, by default, the monitor home page will contain the maximum/minimum computations for measures (i.e., the **Measures At-A-Glance** section). When it is set to **no**, the **Measures At-A-Glance** tab is hidden from the home page, and the **Event Analysis** tab alone appears.

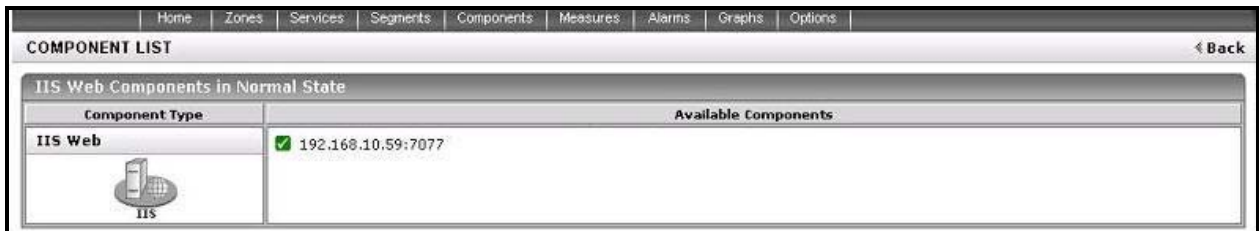
The **Event Analysis** tab page, when clicked, lists the top-5 layers that were most affected by performance issues. Since there are no performance issues in our target environment, the **Event Analysis** tab indicates that no events are currently available.



Figure 3.6: The Event Analysis tab page

Infrastructure Monitoring using eG Enterprise

- The **Components At-A-Glance** section comprises of a bar graph depicting the number of components of each type that are being monitored, and their respective states. Clicking on a bar will take you to a page that lists the individual components of the corresponding type and their current state (see Figure 3.7).



Component Type	Available Components
IIS Web	✓ 192.168.10.59:7077

Figure 3.7: Viewing the list of components of a particular type

Since our target environment comprises of only four component types, the **Components-At-A-Glance** section (see Figure 3.1) will display these types only. Clicking on the **IIS Web** type in Figure 3.1 will reveal Figure 3.7.

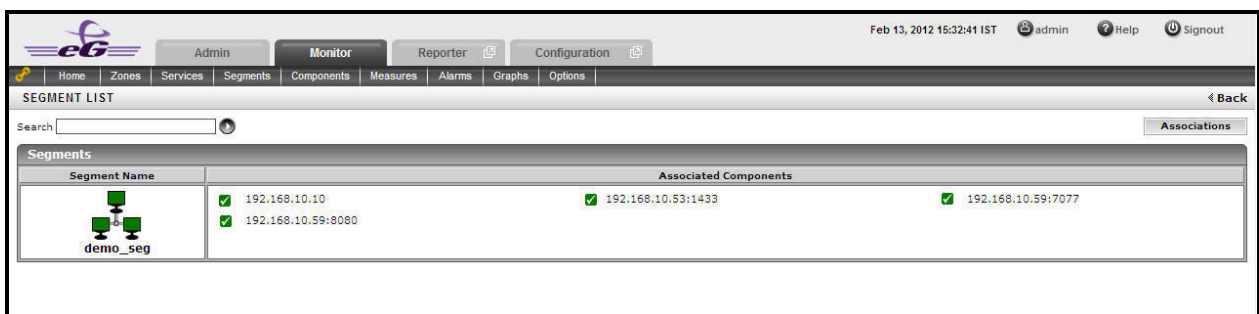
The menu at the top of this page permits monitor users to view the status of the monitored elements such as **Zones**, **Services**, **Segments**, and individual **Components** (see Figure 3.8).



Figure 3.8: The Monitor menu

Selecting the **List** option from the **Zones** menu displays the complete list of zones that have been configured in an environment, and the state of each zone. Since our target environment does not consist of any zone, let us proceed to the **Segments** menu option.

Clicking on the **Segments** menu in Figure 3.8 will reveal a list of segments that have been configured for the target environment; their current state and the components associated with each of the segment (see Figure 3.9).



Segment Name	Associated Components
demo_seg	✓ 192.168.10.10 ✓ 192.168.10.53:1433 ✓ 192.168.10.59:8080

Figure 3.9: The list of segments that have been configured for our target environment

Note that Figure 3.9 displays the only segment configured for our target environment – **demo_seg**, its current state, which is Normal and the components associated with the configured segment.

Clicking on the **Associations** button in Figure 3.9 will reveal Figure 3.10, which displays all the fully configured segments in the target environment, their current state, and the user associated with each of the segments.

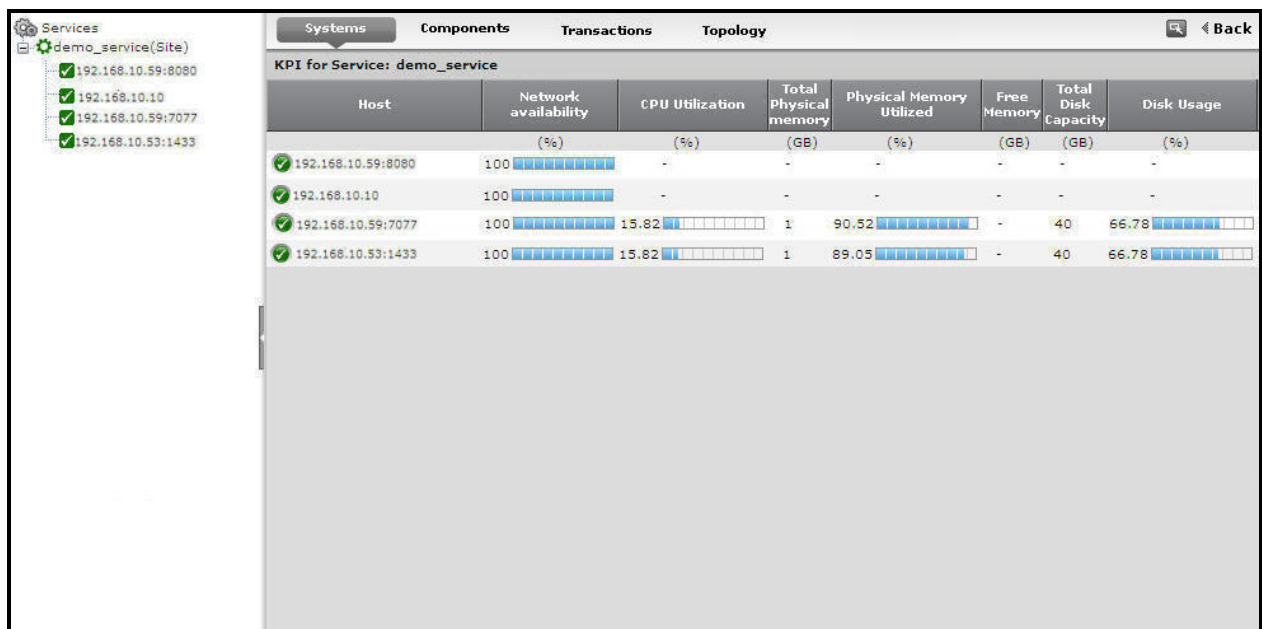
Infrastructure Monitoring using eG Enterprise



Segment	Users
demo_seg	None

Figure 3.10: Viewing the user-segment mappings

Clicking on the **List** option from the **Services** menu in Figure 3.8 will once again bring up Figure 3.2 that lists the services configured in the environment, their current state and the components associated with each of the service. Now when you click on the *demo_service(Site)* under the Services node from the tree structure, a context sensitive right panel will appear displaying the **Service Dashboard**. Figure 3.11 reveals the **Service Dashboard** of the *demo_service(Site)*.



Host	Network availability	CPU Utilization	Total Physical memory	Physical Memory Utilized	Free Memory	Total Disk Capacity	Disk Usage
	(%)	(%)	(GB)	(%)	(GB)	(GB)	(%)
192.168.10.59:8080	100	-	-	-	-	-	-
192.168.10.10	100	-	-	-	-	-	-
192.168.10.59:7077	100	15.82	1	90.52	-	40	66.78
192.168.10.53:1433	100	15.82	1	89.05	-	40	66.78

Figure 3.11: The Service Dashboard that appears when the *demo_service(Site)* is clicked

With this **Service Dashboard**, you will be able to view the host level metrics of the components associated to the service in the **Systems** tab through a single shot. Likewise when you click on the **Components** tab, the application level metrics can be viewed for the associated components of the chosen service. Likewise when you click on the **Transactions** tab page, individual web transactions can be viewed as shown in Figure 3.12.

Infrastructure Monitoring using eG Enterprise

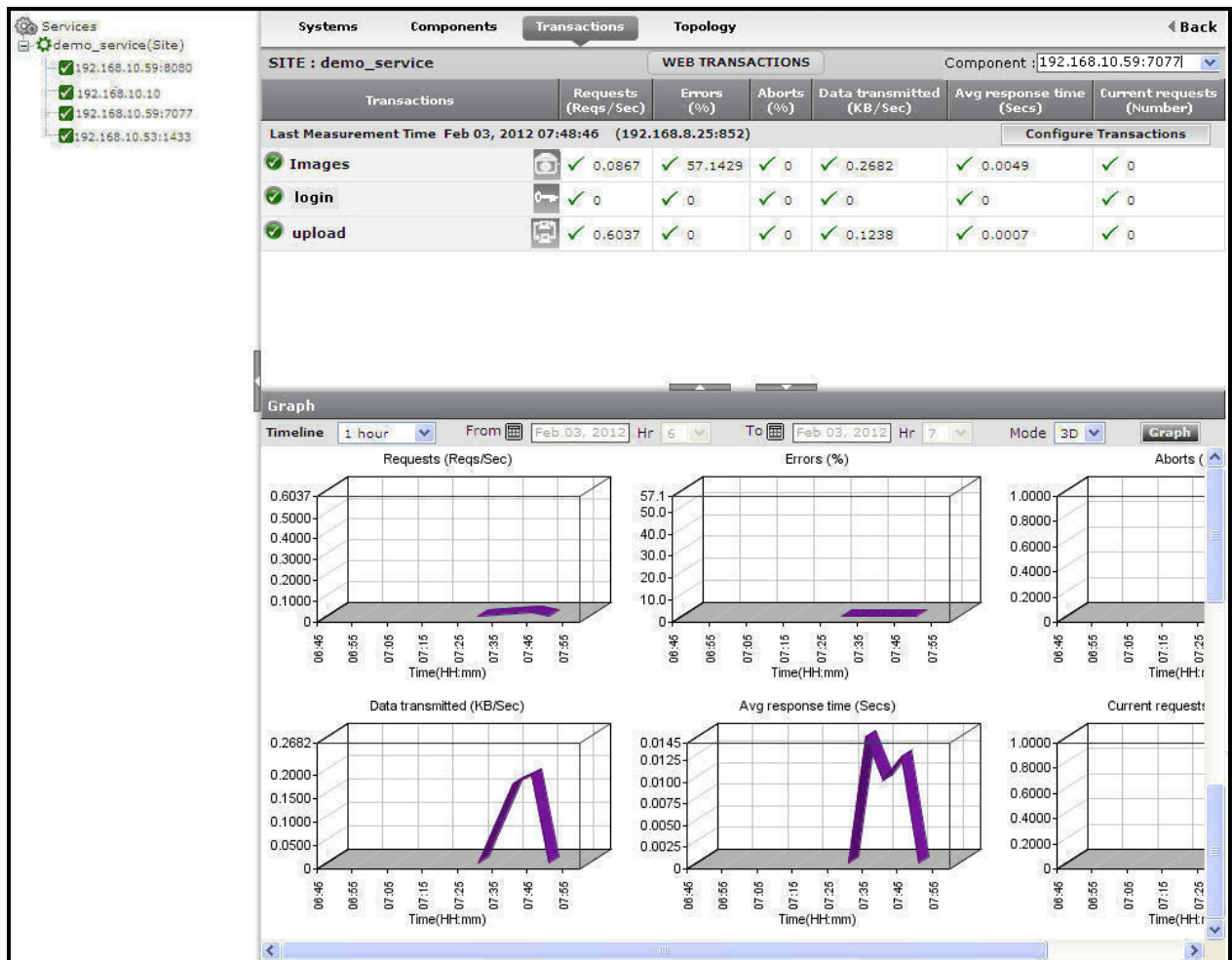


Figure 3.12: The Transaction tab page of the Service Dashboard

This example demonstrates eG's capability to monitor individual web transactions, in real-time. Click on any one of the transactions in Figure 3.12 to view the site topology as in Figure 3.13.

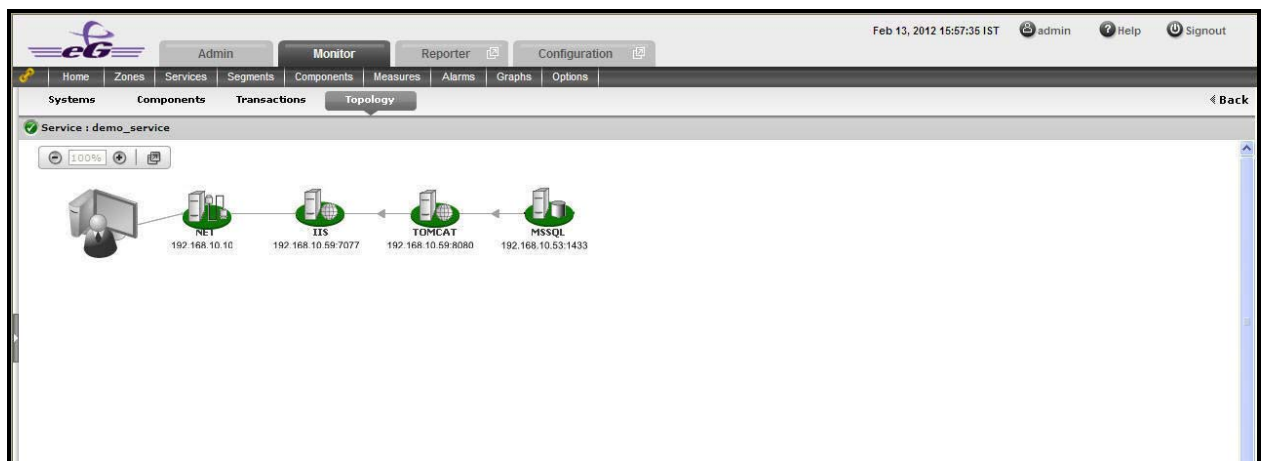


Figure 3.13: The topology of the site demo_service

Infrastructure Monitoring using eG Enterprise

To know more about the **Service Dashboard** and its purpose, refer to the *eG User Manual*.

Click the IIS web server component in Figure 3.13 to view the layers pertaining to it. Figure 3.14 displays the layers of the web server. Click on the **Application Processes** layer. The tests mapping to this layer will be displayed on the right side of the screen. Click on the Processes test and the measures reported by this test appear in the bottom section. The color-coding indicates that there is no problem with any of the measures.

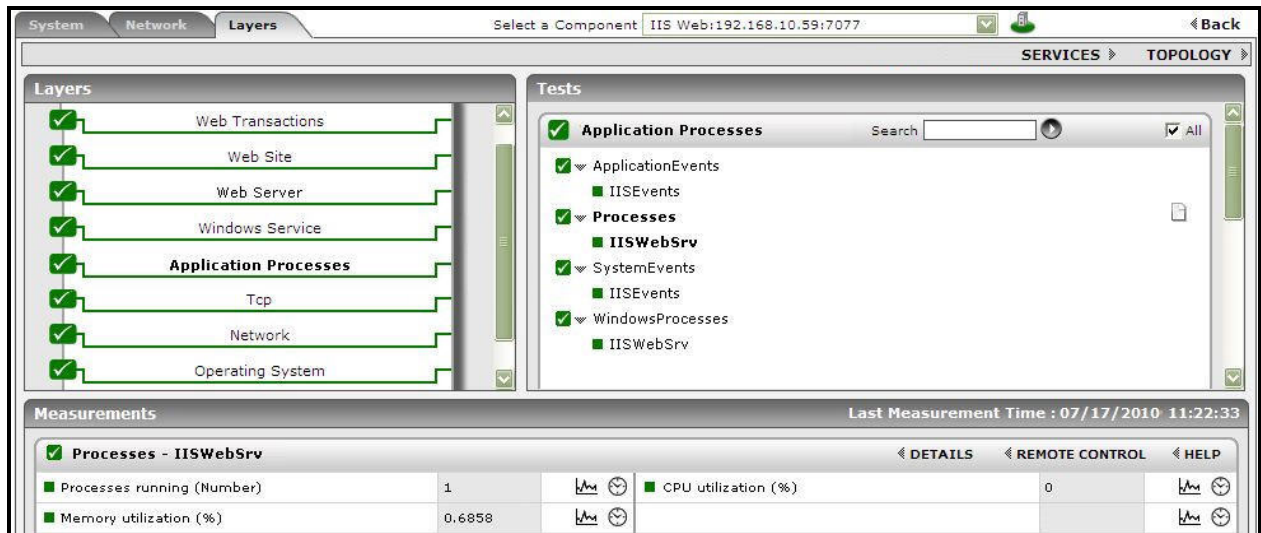


Figure 3.14: Measures pertaining to the Processes Test

eG represents each component as a set of hierarchical layers. The layers of a component are designed such that the state of a layer is impacted by the states of all the layers below it. The state of a layer is dependent on a set of measurements that map to the layer. Figure 3.14 depicts the layer model of an IIS web server, and the tests and measurements that map to its **Application Processes** layer. While a typical IIS web server consists of the **Web Server**, **Windows Service**, **Application Processes**, **Tcp**, **Network**, and **Operating System** layers, an IIS web server hosting a web site that is being monitored will include the **Web Transactions** and the **Web Site** layers. Therefore, if the layer model of an IIS web server is accessed through the topology page (see Figure 3.13), then the **Web Transactions** and the **Web Site** layers will appear additionally.

Figure 3.15 shows the measures reported by the HttpTest for the web server under consideration.

Infrastructure Monitoring using eG Enterprise

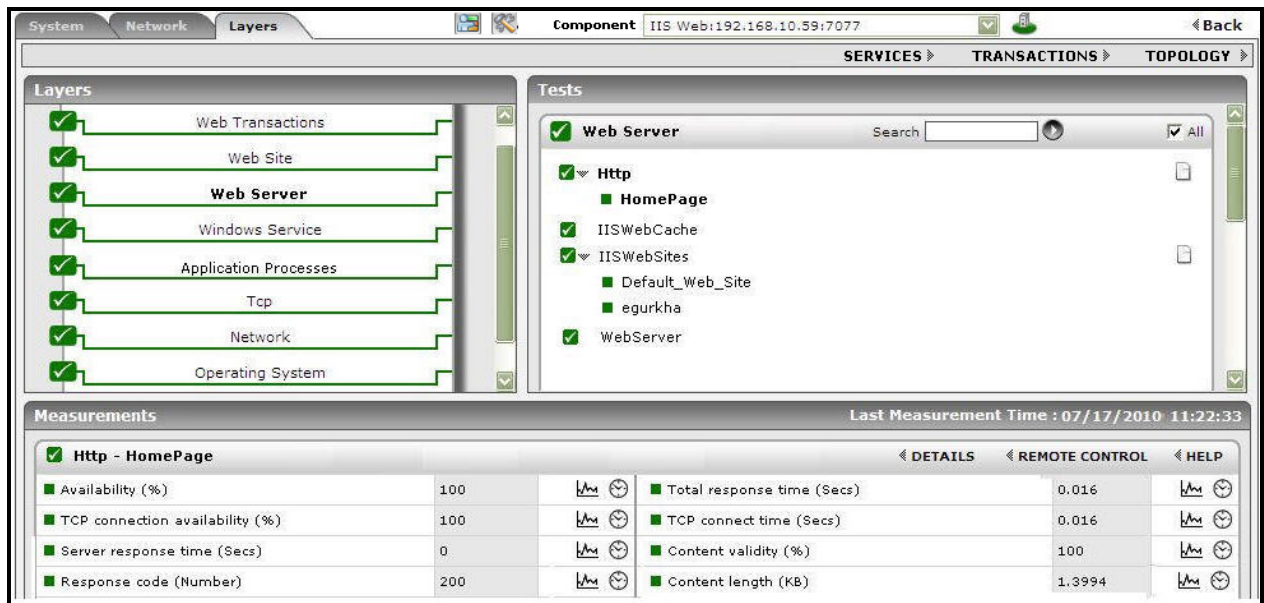


Figure 3.15: Measures reported by the HttpTest for an IIS web server

To create a problem scenario and evaluate how eG Enterprise detects and reports the problem, let us stop the IIS web server running on machine 192.168.10.59 by stopping the World Wide Web Publishing Service through the Services option in the Control Panel. Wait for some time after the web server has been stopped.

Next, move your mouse pointer over the **Alarms** option from the main menu bar, and then, select the **Current Alarms** option from the **Alarms** menu. An alarm window showing the current set of alarms pops up as in Figure 3.16. It is quite evident that both these alarms pertain to the web server component of the web site *demo_service*. However, in the first case the problem is with the **Windows Service** layer and in the second case, it is with the **Web Server** layer.

Show Alarms Filter by Priority Priority All Search by Type						
	TYPE	COMPONENT NAME	DESCRIPTION	LAYER	START TIME	
	IIS Web	192.168.10.59:7077	Service is not up {World_Wide_Web_Publishing_Service}	Windows Service	Dec 31, 2007 15:50	
	IIS Web	192.168.10.59:7077	Web is unavailable {HomePage}	Web Server	Dec 31, 2007 15:51	

Figure 3.16: The eG alarm window

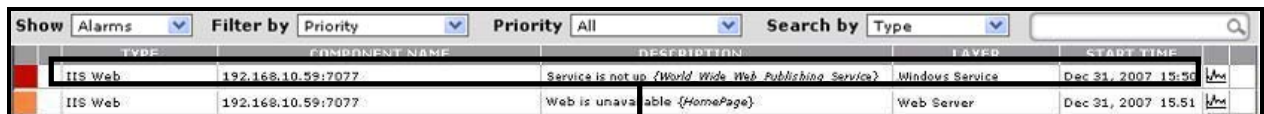
Following conventional management practices, eG Enterprise applies the color-coding scheme mentioned below to indicate alarm priorities:

Color	Priority	Description
Red	Critical	Indicates the existence of a critical issue that requires immediate attention
Orange	Major	Indicates the existence of an issue that could cause serious consequences if not looked into soon.
Pink	Minor	Indicates the existence of a low priority issue. Proactive alerts fall in this category.

Infrastructure Monitoring using eG Enterprise

Accordingly, Figure 3.17 indicates that the eG manager has determined that the critical priority alarm pertains to the **Windows Service** layer. Thus, *by correlating across the different layers* pertaining to the **IIS Web** component, *the eG manager has zoomed in to the root-cause of the problem*, indicating that the failure of the World Wide Publishing Service is causing a problem.

Figure 3.17 below shows how to interpret the contents of the alarm window. Associated with an alarm is the IP address/hostname of the target component, the TCP port number of the component, the layer in the protocol stack that is causing the problem, and the date and time when the problem started.



TYPE	COMPONENT NAME	DESCRIPTION	LAYER	START TIME	
IIS Web	192.168.10.59:7077	Service is not up. (World Wide Web Publishing Service)	Windows Service	Dec 31, 2007 15:50	Graph
IIS Web	192.168.10.59:7077	Web is unavailable (HomePage)	Web Server	Dec 31, 2007 15:51	Graph

Elements of the First Alarm	
IIS Web	Component type
192.168.10.59	IP address
7077	Port number
Windows Service	The Problem layer
Dec 31, 2007 15:50	The Date and time of the problem

Figure 3.17: Contents of the Alarm window

Besides, a **Graph** icon is available against every alarm. Clicking on this icon invokes a graph of the problem measure for the default period spanning the problem date/time and the current date/time (+1 hour). Using this graph, you can observe the time-of-day variations in the behavior of the problem measure.

Moreover, to make diagnosis more efficient and accurate, eG Enterprise embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. For example, when the CPU usage of a host reaches the threshold, the agent can be configured to provide more details – e.g., the top 10 process that are consuming more CPU resources. Optionally, this capability can also be configured to periodically generate detailed measures, regardless of the occurrence of problems.

If the detailed diagnostic capability is enabled for the problem measure indicated by the **CURRENT ALARMS** window, then a special **DD** icon will be available against the corresponding alarm (not shown in Figure 3.17). Clicking on the icon reveals detailed information pertaining to the problem condition, so that you can quickly and accurately zero-in on the root-cause of the problem. For instance, if the **CURRENT ALARMS** window indicates excessive CPU utilization on a host, then against the 'High CPU utilization' alarm in the window, you will find a 'magnifying glass' icon in the **DD** column. Clicking on this icon will list the top-10 CPU-consuming processes executing on the host, thus enabling you to identify the exact process that is causing the issue.

Note:

The **DD** icon will not appear in the **CURRENT ALARMS** window under the following circumstances:

- If the eG license does not support the detailed diagnosis capability
- If detailed diagnosis is not enabled for the test that generates the problem measure
- If no detailed measures are available for a problem test

Move your mouse over the first alarm and you will see the details of the alarm as depicted by Figure 3.18 below. The details include, which test is reporting a problem, and a brief description of the nature of the problem, the association service, and the measurement host. Note that the second alarm pertains to an IIS web server, the problem is the non-availability of the Web server, the associated service is *demo_service*, and the measurement host is the external agent host, *192.168.10.63*.

Show	Alarms	Filter by	Priority	Priority	All	Search by	Type	
	TYPE	COMPONENT NAME	DESCRIPTION	LAYER	START TIME			
	IIS Web	192.168.10.59:7077	Service is not up {World_Wide_Web_Publishing_Service}	Windows Service	Dec 31, 2007 15:50			
	IIS Web	192.168.10.59:7077	Web is unavailable {HomePage}	Web Server	Dec 31, 2007 15:51			
	IIS Web	DESCRIPTION	TEST	SERVICE(S) IMPACTED	MEASUREMENT HOST			
		Web is unavailable {HomePage}	Http	demo_service	192.168.10.63			

Figure 3.18: Viewing the details of the first alarm

Clicking the first alarm in Figure 3.16 will directly take the user to the page shown by Figure 3.19. This figure displays the measure pertaining to the *WindowsServices* test. As is evident from the figure, the **Windows Service** layer is in a **Critical** state, and the **Web Server** layer is in the **Major** state. Figure 3.19 zooms into the **Windows Service** layer and indicates that the *WindowsServices* test is indicating a problem. From the measures, it is clear that the *Availability* is zero. The other two layers on the top are blue depicting that their states are UNKNOWN. This scenario depicts eG Enterprise's **single click diagnosis capability** – by simply clicking on the **Critical** priority alarm, the user is directly led to the root-cause of the problem. The ability to prioritize between alarms and to zoom into the root-cause of problems with very little customization is one of the unique features of eG Enterprise.

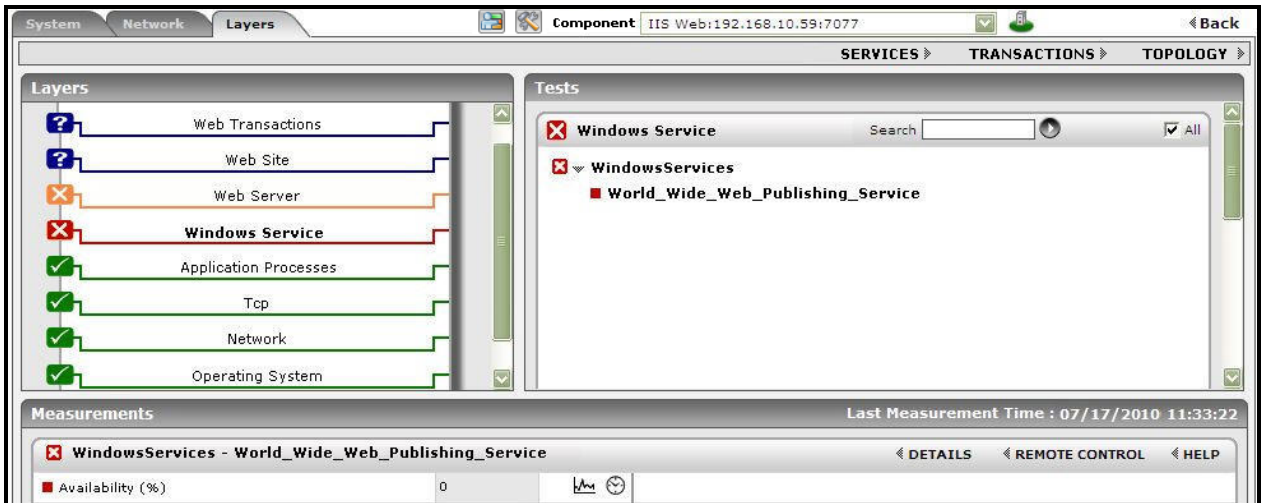


Figure 3.19: Measures pertaining to the WindowsServices test

Similarly, if we look into the **Web Server** layer of Figure 3.20, the Http test is indicating a problem. Looking at the measures reported by this test, we can see that the *Availability* is zero. Moreover, the *Tcp connection availability* is 0, indicating that the Http test failed to even establish a TCP connection to the web server host (possibly because the web server process was not running).

If you view the **CURRENT ALARMS** window (see Figure 3.16) now, you will be able to infer that eG has applied this correlation logic automatically, and has accordingly assigned alarm priorities. In other words, since the root-cause of the problem is the non-availability of the WWW service, the problem with the **Windows Service** layer has been assigned the **Critical** priority. On the other hand, since the problem with the **Web Server** layer is only an outcome of the problem with the **Windows Service** layer, the eG Enterprise system has assigned the **Major** priority to it.

For more details on the measures reported by eG Enterprise tests and their interpretations, click on the **HELP** button in the measurements section of Figure 3.19 and Figure 3.20.

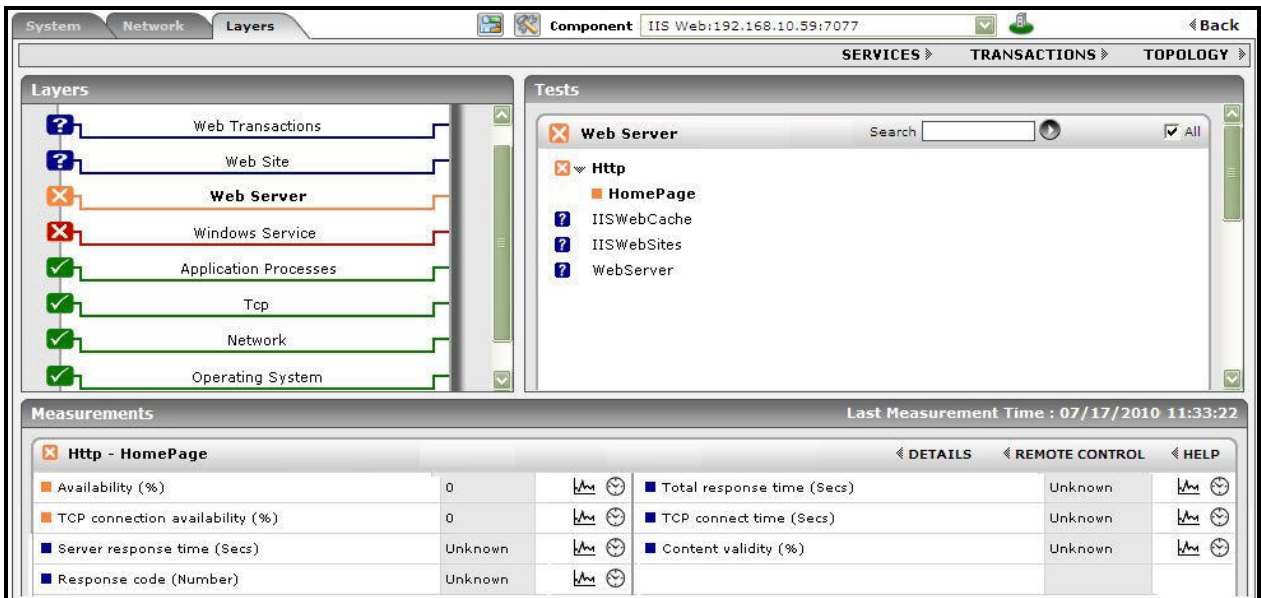
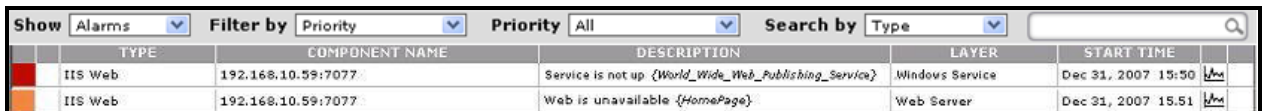


Figure 3.20: Measures pertaining to the Http test

Infrastructure Monitoring using eG Enterprise

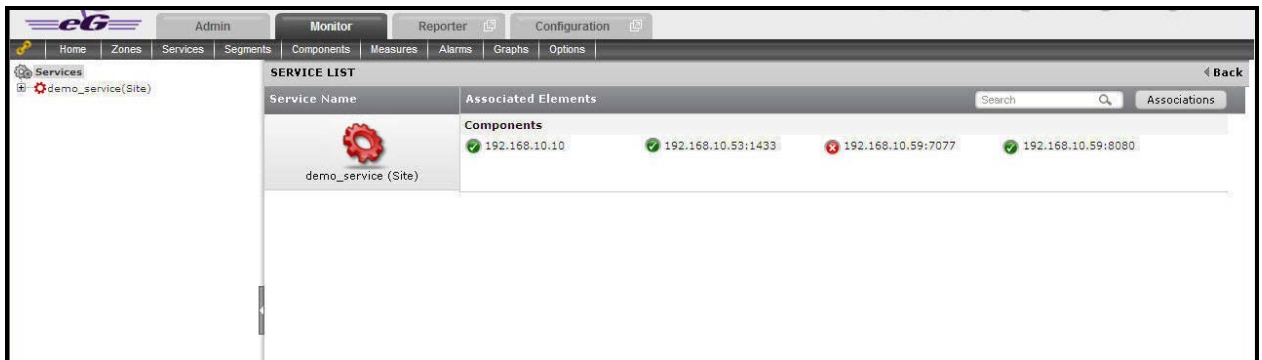
We have so far seen how a *supermonitor* experiences some of the distinct benefits of using eG Enterprise. Let us now proceed to view what the monitor users get to see. Let us take a look from user *john*'s perspective. First log out of the *supermonitor* account using the **Signout** option of the menu depicted by Figure 3.8. Next, we have to login as *john*. For this, specify *john* as the user ID in the Login screen (see Figure 2.3). The password that was given for this user in Figure 2.27 should be next specified in the Login screen. After this, click the **AUTHENTICATE** button to proceed. An alarm window showing a set of alarms shows up as in Figure 3.22. It is quite evident that both these alarms pertain to the IIS web server component of the web site *demo_service* that has been associated with *john*. Clicking on either of these alarms will take the user *john* to the page depicting the measures that are experiencing a problem.



TYPE	COMPONENT NAME	DESCRIPTION	LAYER	START TIME	
IIS Web	192.168.10.59:7077	Service is not up {World_Wide_Web_Publishing_Service}	Windows Service	Dec 31, 2007 15:50	
IIS Web	192.168.10.59:7077	Web is unavailable {HomePage}	Web Server	Dec 31, 2007 15:51	

Figure 3.21: Alarms pertaining to user *john*

Clicking on the **Services** option will reveal Figure 3.22 that lists the services associated with user *john*. Here again, note that the *demo_service* web site associated with user *john* appears and that its state is **Critical**. Also you can view the components that are associated with the *demo_service* service.



Service Name	Associated Elements
demo_service(Site)	Components 192.168.10.10 192.168.10.53:1433 192.168.10.59:7077 192.168.10.59:8080

Figure 3.22: Services associated with user *john*

Now, click on the **Segments** option in Figure 3.8 to view the list of segments associated with user *john*. Since no segments have been associated with the user *john*, the following message appears.

Infrastructure Monitoring using eG Enterprise

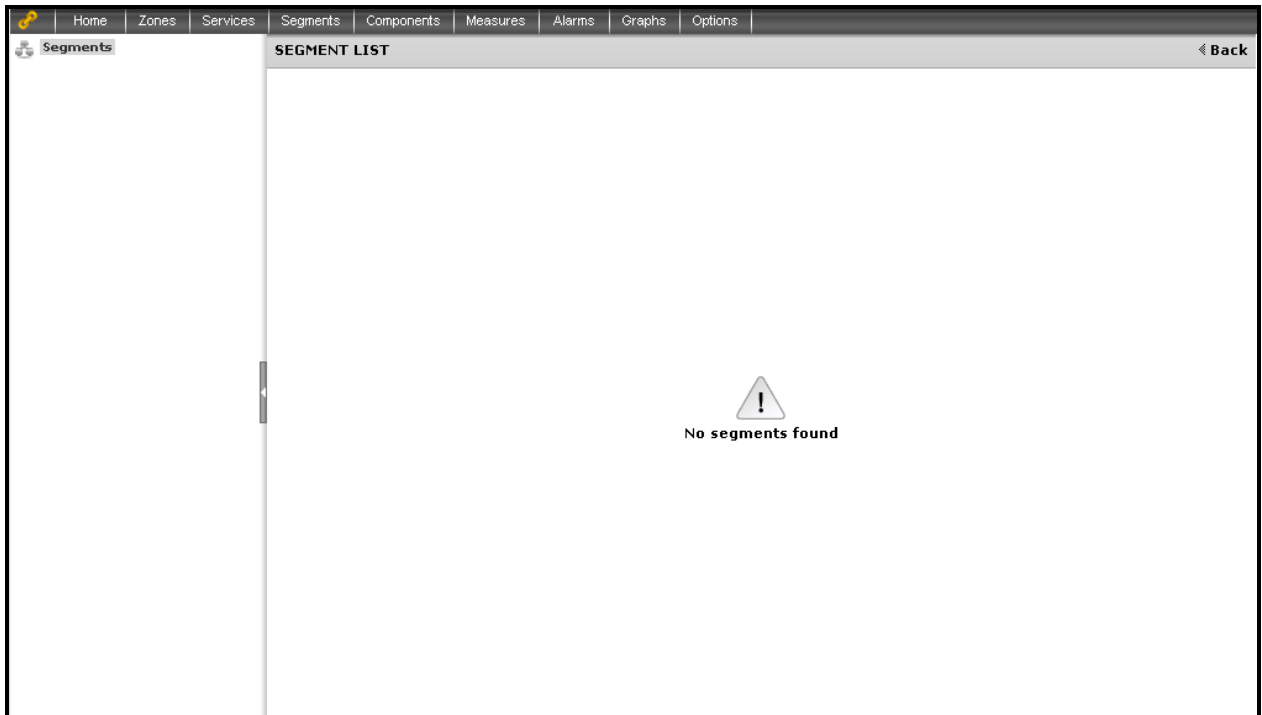


Figure 3.23: A message indicating that no segments have been assigned to user *john*

Thus, the *supermonitor* obtained an unrestricted view of the whole environment, whereas the monitor user's views have been customized to the sites/segments that have been allocated to them.

We have taken a look at a problem scenario that was caused by stopping the IIS web server. Restart the IIS web server. Wait for a few minutes for the eG agent to detect this change in status (This time depends on the frequency of the tests and the alarm policy).

Login as *supermonitor* once again and choose **Current Alarms** from the **Alarms** menu. The alarm window shows that there are no alarms in the environment (see Figure 3.24).

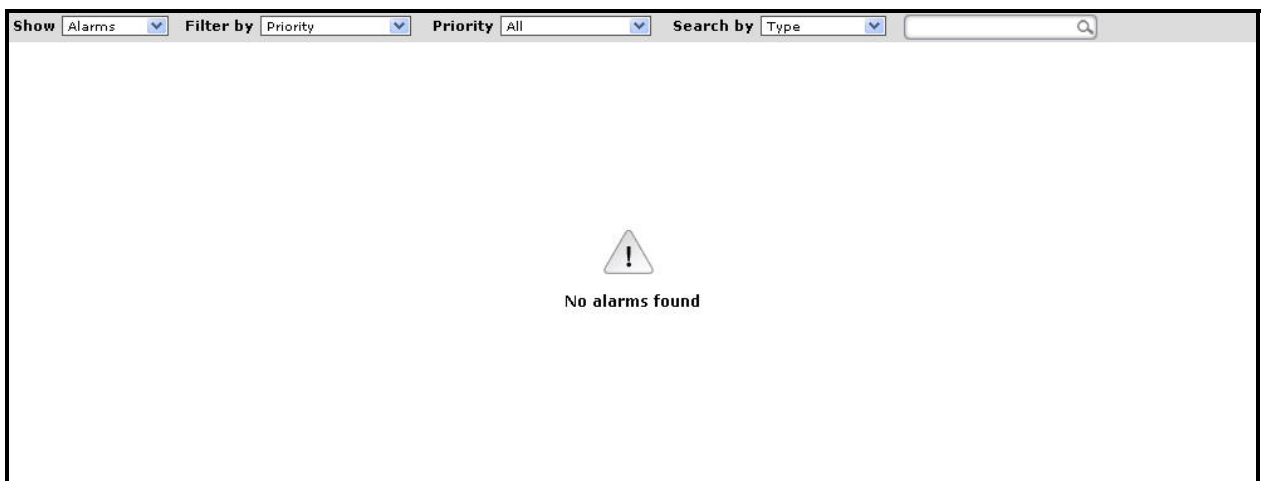


Figure 3.24: Alarm window displaying no alarms

Infrastructure Monitoring using eG Enterprise

The discussion above has illustrated **eG Enterprise's capability to detect and report the root-cause of problems that happen and how it is able to inform users and update itself as and when problems are fixed.**

Finally, to illustrate eG Enterprise's web adapter capability, use a load generation tool such as the public domain *httperf* tool or Microsoft's Web stress test tool. For example, using the *httperf* tool, execute the command

```
httperf --server 192.168.10.59 --port 7077 --uri /index.htm --num-conns 1000000 --rate 20
```

This command results in requests being generated to the demo IIS web server at the rate of 20 requests per second.

Viewing the results of the WebServer test (Figure 3.25), note that the connection rate and the request rate match the load imposed on the web server, thereby proving that eG Enterprise is able to track web server loads effectively.

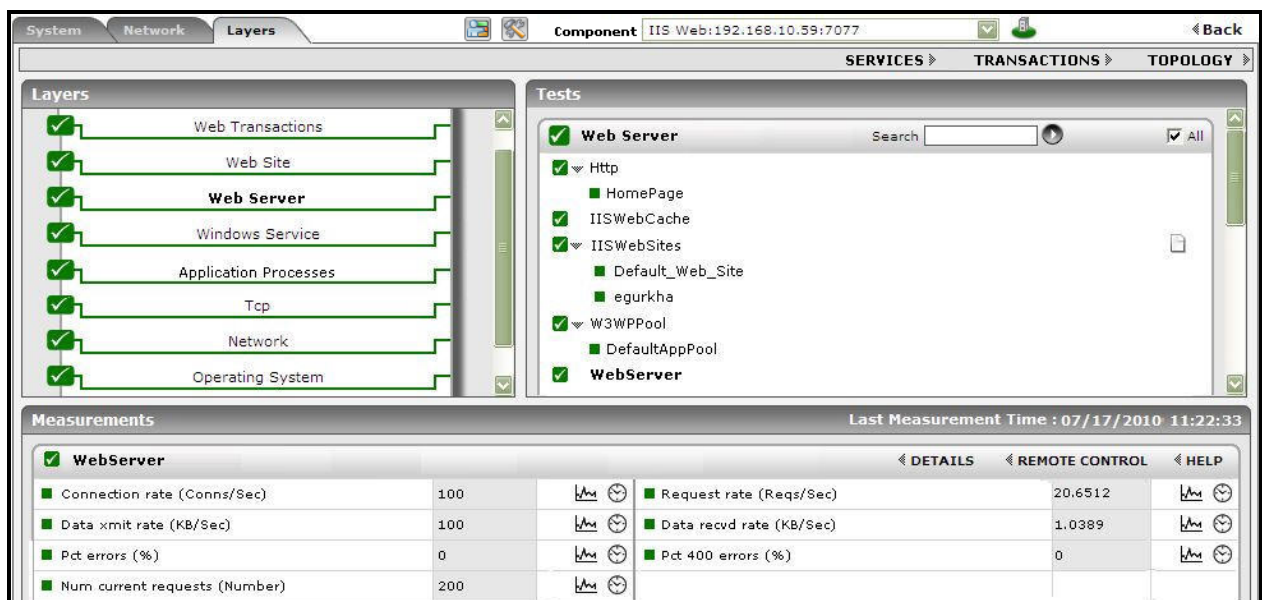


Figure 3.25: Measures reported by the WebServerTest

Conclusions

Using a number of illustrative scenarios, this document has briefly described how a user can set-up and evaluate eG Enterprise. For more details regarding using eG Enterprise, the interested reader is referred to the other *eG Manuals*.

Index

A

A Description of the Target Environment.....	3
Administering the eG Suite	
Adding New Users	27
Configuring Components	
Adding Components.....	13
Changing preferences	9
Configuring the segment topology.....	18
Discovering Components	9
Managing Components	12
Configuring Tests	34
Configuring the Java Server Web AccessTest.....	38
Configuring the Network Interfaces Test.....	42
Configuring the ProcessTest	41
Configuring the SQL Database SpaceTest.....	38
Configuring the SQL Network Test.....	35
Configuring Web sites.....	21
Configuring transactions	24

I

Infrastructure Monitoring using the eG Suite	
--	--

A supermonitor's view.....	44
Demonstrating eG's graphing capabilities	59
Illustrating eG's web adapter capability.....	59
User john's view	57
Installing and Configuring eG Agents	
Configuring the eG web adapter capability.....	43

S

Steps for deploying the eG Suite	
Administration	2
Installation and Configuration	2
Monitoring	2
Steps for Installing and Configuring eG Agents	43
Installing and Configuring an eG agent.....	43
Starting the eG agent.....	43
Steps for installing and configuring the eG Manager	
Installing and Configuring the eG manager	4
Starting the eG manager	4
Verifying prerequisites	4
Steps for installing and configuring the eG Manager.....	4